Enterprise Resilience

Prepare.

Why Enterprise Resilience Matters

Compete.

Council on Competitiveness

Why Enterprise Resilience Matters

EDITED BY Debbie van Opstal, Senior Vice President, Policy and Programs, Council on Competitiveness

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 us at www.compete.org.

DESIGN Soulellis Studio

Enterprise Resilience

Prepare.

Why Enterprise Resilience Matters

Prepare.
Table of Contents

Foreward by Deborah L. Wince-Smith

These first years of the 21st century are best described by three Ts: transition, turbulence and transformation. Rapid globalization is altering our world in fundamental ways, and we are more connected and more interdependent than ever before. Risks are magnified in an environment in which disruptions cascade across networks and borders. What happens anywhere can have profound effects everywhere.

Countries, communities and companies face what professor Anthony Giddens called the new "riskiness to risk." The impact of point failures, whether triggered by attack or accident, can reverberate quickly across networks—and failure to anticipate and adapt to turbulence can cascade into a "bet the company" mistake. An Economist Intelligence Unit survey found that one in five companies suffered significant damage from risk failures. Yet, only 25 percent of companies set regular risk targets for managers, and less than one-third provide risk management training. Some companies remain in the dark about the risks they face. Nearly half of the respondents to a Deloitte survey stated that their company's non-financial reporting measures were ineffective or highly ineffective in shaping the decision-making process.

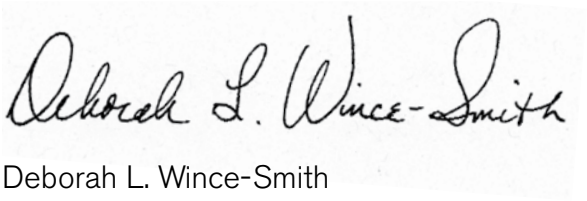
Prepare represents the thought leadership of a group of C-suite executives and resilience experts who met for a day and half at a Risk Intelligence and Resilience Workshop in Wilmington, Delaware. It was initially developed as a briefing book for workshop participants on seminal research and recommendations in the fields. It now includes the summary of their discussions representing the insights of those participants, who collectively represent over a millennium of risk management experience.

A key conclusion: The next new revolution in business will be in risk management and resilience. Just as we built integrated quality and safety management systems, so we must now build integrated risk management systems. Enterprise resilience is an approach to risk management that anticipates disruptions, better ensures recovery and protects business profitability. Risk-intelligent organizations elevate resiliency to a board-level concern and bake it into the DNA of their enterprise with powerful processes, well-trained people and robust systems. Their goal is to be proactive and adaptive in response to disruptions, whatever form they take. Resiliency goes beyond minimizing losses to include preserving shareholder value, finding competitive advantage in the ability to manage risk well and growing the top line.

For countries, resilience has replaced the three Gs—guards, gates and guns—as the national strategy. Our work has inspired the government to focus on resilience instead of protection, with the creation of a Resilience Directorate in the National Security Council. We see the need for continuing dialogue between the public and private sectors that lever-

ages resilience to meet multiple goals of national security, homeland security, energy security and economic competitiveness.

I would like to thank James H. Quigley, CEO of Deloitte, and John Swainson, former CEO of CA Inc., for their sponsorship of this opportunity to understand how different risk functions link to each other and to strategic planning, and what CEOs and boards need to know about risk management. Mark Layton, vice chairman of Deloitte; Vikram Mahidhar, director of operations of Deloitte Research; and Margaret Brooks, vice president at CA Inc.; provided advice and insights on an ongoing basis. At the Council, senior vice president Debra van Opstal ably led the Council team, with the help of David Padgham, Mildred Porter and Michael Ruthenberg-Marshall.



Deborah L. Wince-Smith
President and CEO
Council on Competitiveness

Agenda

October 30, 2009

12:00 Welcome and Introductions
Lunch

12:30 Setting the Global Stage

Warning! Turbulence Ahead: Strategic Risks

Erik Peterson
Director
Global Strategy Institute
Center for Strategic and International Studies

1:30 The Risk-Intelligent Enterprise

Rick Funston
Principal and National Practice Leader for Governance and Risk Oversight
Deloitte & Touche, LLP

2:15 What Risk Executives Think: Survey Results

Vikram Mahidhar
Senior Manager, Deloitte Research
Deloitte & Touche, LLP

2:45 Session 1
Words Matter: Defining Risk Intelligence and Resilience

Creating a Common Lingo. The terms risk intelligence and resilience actually mean different things to different people—spanning a spectrum from disaster management preparations to fences and firewalls; from business continuity to competitive advantage. Words matter—and we need to create a common language of risk.

Goal: The overall goal is not so much to achieve perfect definitions of "resilience" and "risk intelligence" as it is to get insights from the participants on how they operationalize these objectives in their own organizations.

Paper Presentation
Erica Seville
University of Canterbury
New Zealand

Commentators
Mary Herbst
Director of Business Resiliency
Carlson Hotels

Anne Larsen
Advisor, Corporate Responsibility
Novo Nordisk A/S

Darren Mulholland
Senior Vice President, Operations and Technology, NASDAQ

3:45 Breakout Sessions: Defining the Desired State

Agenda

5:00 **Reports from the Breakouts: Defining Risk Intelligence & Resilience**

Co-Chairs for Breakout and Reports:

Breakout 1

Bob Moore
Vice President, Global Security Group, HP

Carl Gibson
Director, Risk Management Unit, Latrobe University, Australia

Breakout 2

Joe Petro
Managing Director, Citigroup

Joseph Fiksel
Executive Director, Center for Resilience
Ohio State University

Breakout 3

Jim Porter
Vice President and Chief Engineer
DuPont (ret.)

Bob Flynn
Vice President, Travelers

Breakout 4

Ken Senser
Senior Vice President
Global Security, Wal-Mart, Inc.

Branko Terzic
Senior Energy Consultant, Deloitte

5:30 **Break**

6:00 **Reception**

6:30 **Dinner**

7:30 **Evening Discussion: What should managers and directors be asking about risk?**

Moderator
Deborah L. Wince-Smith
President
Council on Competitiveness
Director, NASDAQ

Tom O'Neill
Principal, Sandler O'Neill
Chair, Audit Committee, ADM

Larry Rittenberg
Chairman of COSO
Ernst & Young Professor of Accounting & Information Systems
University of Wisconsin

Mark Layton
Global Leader, Enterprise Risk Services and Vice Chairman, Audit
Deloitte & Touche, LLP

The Honorable Roy Ferguson
New Zealand Ambassador

9:30 **Adjourn**

October 31, 2009

7:30 Networking Breakfast

8:30 A CEO's Perspective on Risk
Conversation with Charles O. Holliday, Jr., CEO, DuPont

9:00 Session 2
Numbers Matter: Metrics for Risk Intelligence and Resilience

Developing a Dashboard: Once a common language of risk is developed, metrics are needed that cross risks and functions to accurately assess enterprise risk—existing as well as emerging risks — or determine whether management objectives have been achieved.

Goal: The goal is to identify measures of risk that are meaningful to management, comparable across risk management functions, and explicitly tied to enterprise objectives and performance.

Paper Presentation

Brian Ballou/Dan Heitger
Co-Directors, Center for Business Excellence
Miami University of Ohio

Commentators

Spiros Dimolitsas
Senior Vice President, Georgetown University

John O'Connor
Director of Supply Chain Risk Management
Cisco Systems, Inc.

Pat Gnazzo
Senior Vice President, U.S. Public Sector Business, CA Inc.

10:00 Breakout Sessions
Measuring Risk Intelligence and Resilience

11:30 Reports from Breakout Groups

Co-chairs for Breakouts/ Reports:

Breakout 1

Bobbi Bailey
Vice President, Global Network Operations

Jane Carlin
Global Head of Operational Risk, BCP, and Information Security, Morgan Stanley

Breakout 2

Steven Trevino
Managing Director
Resilient Civilization Initiative

Chris McIlroy
Director, Infrastructure Protection & Resiliency Division, SRA International, Inc.

Breakout 3

Judith Cardenas
CEO, Center for Performance and Accountability; and Vice President, University Center, Lansing Community College

Bill Raisch
Director, International Center for Enterprise Preparedness

Breakout 4

Scott McHugh
Vice President, Global Asset Protection
Wal-Mart

Steve Spoonamore
Partner, GSP LLC

12:00 Networking Break/Luncheon Buffet

12:30 Roundtable on Recommendations: Policies and Practices that Support Risk Intelligence and Resilience

Questions for Discussion: The evidence seems to indicate that companies which are more risk intelligent and resilient outperform the market. If that's true, why don't the markets reward companies that demonstrate risk intelligence and resilience? What role could the ratings, insurance and audit industries play in creating incentives/ requirements for risk management? What should government do to encourage these market movers to reward resilience? What should government do to protect citizens from the consequences of massive failures in risk management?

Goal: To identify how the markets can incentivize better risk management practices, particularly through ratings, insurance and audit, and what government can do to strengthen and complement market incentives.

Moderator
Henry Ristuccia
Partner
Deloitte & Touche, LLP

Linda Conrad
Director, Customer Enterprise Risk Management, Zurich

Christine St. Clare
Advisory Partner, KPMG

Phil Auerswald
Professor of Public Policy, George Mason University

2:45 Next Steps

3:00 Adjourn

Rick Funston, Deloitte & Touche, LLP

The Risk-Intelligent Enterprise

Rick Funston
Principal and National Practice Leader, Governance and Risk Oversight
Deloitte & Touche, LLP

The ability to survive and thrive in an uncertain and turbulent environment requires resilience and agility. Resilience is the ability to rapidly recover and resume a former shape. Agility is the ability to assume a desired shape in order to rapidly adapt and seize desired opportunities. Risk intelligence is the ability to detect and rapidly respond to changes that affect the business model and bottom line.

Risk Intelligence enables:

- No surprises
- No big mistakes
- No missed opportunities

Of course, brutal reality is that there will always be surprises, mistakes and missed opportunities. But, in a risk-intelligent enterprise, they will not be life-threatening.

Critical Skills of Risk-Intelligent Enterprises

Check Your Assumptions at the Door. It is better to be roughly right than precisely wrong. Risk-intelligent enterprises look for evidence that their assumptions are wrong. Sometimes that means identifying weak signals that key assumptions in your environment are changing in ways that threaten your business.

Anticipate Potential Causes of Failure. It is almost un-American to think of failure, but risk-intelligent enterprises legitimize a constructive discussion of triggers for failure. They do not just step outside the box, they actively attack it.

Identify Interconnections and Interdependencies. The weakest links are often at the nexus of core processes.

Improve Reaction Time. One of the distinguishing aspects of turbulence is speed—most companies do not factor velocity into their risk assessments. Bad things happen faster

than good; reputations are gained in inches per year and lost in feet per second. The speed of response has to be matched to the speed of onset.

Develop Common Senses to Get Insight and Foresight, Not Hindsight. Most enterprises tend to lack a central risk nervous system and good communications lines between multiple appendages. Specialist functions speak specialty languages and have a hard time communicating with one another, with the result that enterprise communications can become a tower of Babel. And, management structures sometimes act as buffers to prevent bad news from getting to the corporate brain. Honing the common senses that identify over-the-horizon risks require enterprise collaboration and communication.

Verify Sources of Information. In God we trust; all others bring data. Prior experience is not necessarily a good predictor for the future. Executive opinions, while important, need to be corroborated.

Maintain a Margin of Safety. October is a particularly dangerous month to invest in stocks. Other dangerous months are July, January, September, May, March, November and so on. According to Warren Buffet, the most dangerous words in the investors lexicon are "everyone else is doing it."

Maintain Operational Discipline. For mountaineers, most accidents happen on the way down. Attention should be constantly focused on operational discipline.

Adopt a Long-Term View. Urgent problems are often not the most important ones. And short term events carry a risk of over-reaction. Risks have to be taken to sustain ROI.

In sum:

- Build risk intelligence into decision-making processes, but do not bolt it on.
- Focus on value—protecting what you have while creating new value.
- Drive out fear of talking about potential for failure.
- Generate dialogue, not reports.
- Rely on judgment, not formulas.
- Manage icebergs first, not ice cubes.

Workshop Summary

Words Matter: Defining a Common Vocabulary

The language we use matters. Often we use the same words to mean different things. Or, the words we use describe qualities, not competencies. The lack of a common language of risk is one of the chief barriers to risk intelligence and resilience. We need common understandings about the words we use to communicate effectively with each other, with our management, with our investors and even with our regulators.

Resilience: Great Concept…but What Does It Mean?

Erica Seville
Research Fellow
University of Canterbury, New Zealand

Resilience is about an organization's ability to achieve its core objectives, even in times of adversity, so that it survives in good times AND in bad. Resilient organizations are able to cope with both the foreseeable events that are on their risk radars, and the ones that come out of the blue.

Seizing Opportunity: Resilience is not just about survival, but the ability to seize opportunity out of crisis. There are always opportunities in a crisis, and the organizations that are able to seize these opportunities for renewal are the ones that will both survive and thrive. The qualities that enable an organization to survive in adversity are the same qualities that enable it to compete successfully on a day-to-day basis. The case for resilience is about market leadership as well as crisis management.

Interdependencies: Another key characteristic is that resilience cannot be achieved by any one organization. No organization is an island. It operates within a network of other organizations which, if not also resilient, could eventually pull down the network. We need to raise the game of all the organizations in the network. Equally important are resilient communities. Organizations are only as resilient as their people and the communities in which they live.

Dynamic: Resilience is dynamic, not static. Every time an organization implements a new technology or has a fractious round of pay negotiations, it is shifting its resilience space. One-time resilience audits do not work—resilience needs to be constantly re-evaluated.

Resilience is an overarching concept that pulls together many aspects of good business management. It forces business leaders to think about, anticipate and plan for those things that are not on the risk radar—and to develop adaptive management strategies.

Four pillars of resilient organizations include:

- **Resilience Ethos:** How well has the organization built a value system and culture that sets resilience as a goal? Has it made the effort to build wider networks for resilience?
- **Situational Awareness:** Does the organization have its finger on the pulse of its operating environment. Is it positioned to recognize subtle shifts, identify potential opportunities and threats, and mobilize itself to respond?

Erica Seville, University of Canterbury, New Zealand

- **Processes for Managing Keystone Vulnerabilities:** Does the organization know where its critical vulnerabilities are and how proactively it is managing them?
- **Adaptive Capacity:** When the chips are down and the plan did not work, how well can the organization come up with new strategies and implement them rapidly?

Finally, there is no one model for resilience. Like individuals, organizations have their own personalities, strengths and weaknesses. The key is to make the most of strengths in times of crisis and understand weaknesses, and hopefully shore them up before the crisis moment comes.

Table 1: Defining Resilience Using a Competencies Framework

Resilience Ethos: A culture of resilience that is embedded within the organization across all hierarchical levels and disciplines, where the organization actively manages its position in an interdependent system and where resilience issues are key considerations for all decisions that are made.	
INDICATOR	**DEFINITION**
Commitment to Resilience	A belief in the fallibility of existing knowledge as well as the ability to learn from errors as opposed to focusing purely on how to avoid them. It is evident through an organization's culture, training and how it makes sense of emerging situations.
Network Perspective	A culture that acknowledges organizational interdependencies and realizes the importance of actively seeking to manage those interdependencies. It is a culture where the drivers of organizational resilience and the motivators to engage with resilience are present.

Situation Awareness: An organization's understanding of its business landscape; its awareness of what is happening around it, and what that information means for the organization, now and in the future.	
INDICATOR	**DEFINITION**
Internal and External Situation Monitoring and Reporting	The creation, management and monitoring of human and mechanical sensors that continuously identify and characterize the organization's internal and external environment, and the proactive reporting of this situation awareness throughout the organization.
Informed Decision Making	The extent to which the organization looks to its internal and external environment for information relevant to its organizational activities and uses that information to inform decisions at all levels of the organization.
Recovery Priorities	An organization-wide awareness of its priorities following a crisis, clearly defined at all levels of the organization, as well as an understanding of the organization's minimum operating requirements.
Understanding and Analysis of Hazards and Consequences	An anticipatory all-hazards awareness of any events or situations which may create short or long-term uncertainty or reduced operability. An understanding of the consequences of that uncertainty to the organization, its resources and its partners.
Connectivity Awareness	An awareness of the organization's internal and external interdependencies and an understanding of the potential scale and impact that expected or unexpected change could have on those relationships.
Roles & Responsibilities	Roles and responsibilities are clearly defined and people are aware of how these would change in an emergency, the impact of change, and support functions it requires.
Insurance Awareness	An awareness of insurance held by the organization and an accurate understanding of the coverage that those insurance policies provide. (Note: This indicator seems at a more micro-level than others, but we regularly observed organizations using insurance as a security-blanket, without a good understanding of the limitations of that cover!)

Management of Keystone Vulnerabilities: The identification, proactive management, and treatment of vulnerabilities that, if realized, would threaten the organization's ability to survive.	
INDICATOR	**DEFINITION**
Robust Processes for Identifying and Analyzing Vulnerabilities	Processes embedded in the operation of the organization that identify and analyze emerging and inherent vulnerabilities in its environment, and enable it to effectively manage vulnerabilities to further the networks' resilience.
Planning Strategies	Effectiveness of organizational planning strategies designed to identify, assess and manage vulnerabilities in relation to the business environment and its stakeholders.
Participation in Exercises	Participation of organizational members in rehearsing plans and arrangements that would be instituted during a response to an emergency or crisis.
Capability and Capacity of Internal Resources	The management and mobilization of the organization's physical, human, and process resources to effectively respond to changes in the organization's operating environment.
Capability and Capacity of External Resources	Systems and protocols designed to manage and mobilize external resources as part of an interdependent network to ensure that the organization has the ability to respond to crisis.
Organizational Connectivity	Management of the organization's network interdependencies and the continuous development of inter-organizational relationships to enable the organization to operate successfully, and to prevent or respond to crisis and uncertainty.
Staff Engagement and Involvement	The engagement and involvement of staff so that they are responsible, accountable and occupied with developing the organization's resilience through their work because they understand the links between the organization's resilience and its long term success.

Adaptive Capacity: The organization's ability to constantly and continuously evolve to match or exceed the needs of its operating environment before those needs become critical.	
INDICATOR	**DEFINITION**
Strategic Vision and Outcome Expectancy	A clearly defined vision which is understood across the organization and reflects its shared values and empowers its stakeholders to view the organization's future positively.
Leadership, Management and Governance Structures	Organizational leadership which successfully balances the needs of internal and external stakeholders and business priorities, and which would be able to provide good management and decision making during times of crisis.
Minimization of Silo Mentality	Reduction of cultural and behavioral barriers which can be divisive within and between organizations, which are most often manifested as communication barriers creating disjointed, disconnected and detrimental ways of working.
Communications and Relationships	The proactive fostering of respectful relationships with stakeholders to create effective communications pathways which enable the organization to operate successfully during business-as-usual and crisis situations.
Information and Knowledge	The management and sharing of information and knowledge throughout the organization to ensure that those making decisions or managing uncertainty have as much useful information as possible.
Innovation and Creativity	An organizational system where innovation and creativity are consistently encouraged and rewarded, and where the generation and evaluation of new ideas is recognized as key to the organization's future performance.
Devolved and Responsive Decision Making	An organizational structure, formal or informal, where people have the authority to make decisions directly linked to their work and, when higher authority is required, this can be obtained quickly and without excessive bureaucracy.

Anne Gadegaard Larsen, Novo Nordisk

Resilience and Sustainability

Anne Gadegaard Larsen
Specialist, Corporate Responsibility Management
Novo Nordisk

Words do matter. For example, we are doing many of these things in our company, but no one would call it resilience. Our focus has been on stakeholder engagement. Many defining moments have come from a failure to pay attention to what stakeholders were thinking. Historically, that is partially because companies tend to see themselves as the center of events relevant to their stakeholders. But, in this complex world, many of the issues important to stakeholders may actually be beyond a company's direct control.

At Novo Nordisk, the triple bottom line means managing at the borderline between societal challenges and business. We have to address issues that are important to our stakeholders by bringing all the best ideas and competencies of the company to bear and to ensure that these issues are included in our decision-making processes. About 10-15 of our top 100 risks are non-financial.

We believe that stakeholder engagement and partnership is a key element in assuring growth and long-term sustainability. For example, 85 percent of our energy consumption is in Denmark. Consequently, we have partnered with a large energy producer which is helping us identify energy savings. We are banking the savings with a commitment to purchase green electricity when the producer has built enough windmills to provide it. A win-win solution for us—we have reduced our carbon emissions—and for them.

Resilience at NASDAQ

Darren Mulholland
Senior Vice President, Operations and Technology
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. It processes more than 230 million transactions daily at a rate of 64,000 transactions per second. In the time it takes to read this sentence, NASDAQ will process nearly 200,000 transactions. NASDAQ has been learning how to deal with a tumultuous environment since 9/11 and has developed a number of best practices to cope. Just in terms of volume group, our transactions volume have doubled—not just daily but on a second-to-second level—which is great for the business but creates some enormous capacity problems. We have had to build an agile, operational environment that affords us the flexibility to respond to those types of capacity demands instantly.

Perfection is unattainable. We operate from the perspective that never going down is impossible. So, we focus on agility—a capability to bring up systems and data centers within seconds. Our biggest challenge is not internal, but in the financial market community. It is not the norm to be able to operate with agility in such a highly regulated environment.

Mary Herbst, Carlson Hotels Worldwide

Business Resiliency: Moving the Mountain an Inch at a Time

Mary Herbst
Former Director of Business Resiliency, Audit and Business Risk Management
Carlson Hotels Worldwide

Carlson is in the hospitality business, with facilities all over the world known under several brand names from the Raddison Hotels to TGIF. We operate in some high-risk areas, so we need to be able to understand those risks and prepare crisis plans. In times of crisis, we need to make sure that our employees know what to do to keep our guests safe and to minimize the chaos. What is less understood is that we also provide shelter and food in times of disaster—for those evacuated as well as for relief teams. After Hurricane Katrina, our TGIF restaurant was up and running in 24 hours, serving $2 meals and $3 beers and providing complementary meals to those who could not pay. We provided showers and daycare for employees and others. Importantly, that store is also our No. 1 producer in the nation and in the world because of its rapid response and community ties.

Carlson created a Business Resilience Council comprised of representatives from all of the business units as well as the financial, HR and PR areas. In the event of a disaster, the Council could be convened in conjunction with the crisis team. We need to have processes, plans and standards in place, but we also need commitment to the mission. Complacence often sets in when a few years pass without an event. And, without an ongoing effort, your processes, policies and plans are only as good as your last crisis, not your next. We have to take resilience from theory to reality. Our goals are to ensure that our guests and employees are safe, evaluate and secure our site quickly in the event of crisis, respond and resume business quickly, and understand our end-to-end risks and how to mitigate them.

Key Observations from the Discussions

Define Resilience: Resilience is a process of preparation, implementation and lessons learned. It is a framework, a process and a lifecycle—a constant evaluation of where you are in relationship to your business objectives and risks.

- Resilience is a steward of—and a way to "future-proof"—business strategy.
- Resilience is fleeting. The level of resilience an organization achieves today could be gone tomorrow. Changing contexts create new resilience challenges.
- Resilient organizations are prepared to reinvent themselves. In a period of change, they do not go back to old ways of doing things, but adapt and evolve.
- The rewards of resilience are both financial and intangible—brand, reputation and relationships. An organization's survival is closely tied to these intangibles.

Define Risk Intelligence: Deloitte coined this term because of the confusion in marketplace and the alphabet soup—from ERM (enterprise risk management) to CM (crisis management) to GRC (governance, risk and compliance)—that was floating around. Risk intelligence is an aspirational state of continuous improvements in risk management and governance.

Risk Intelligence Before Resilience: Risk intelligence is the information needed to make an organization resilient. It is not just the ability to see what is ahead, but what is around the corner. It is knowledge, foresight, pervasive situational awareness and the ability to communicate risks. An organization needs to be risk intelligent before it can develop the capacity to be resilient.

Ignore Definitions, Focus on Process: It does not look like there will ever be a common language of risk. Focus on common processes rather than a common lingo.

Focus on the Ecology of Risk: Organizations tend to look inward to manage risk when they should be looking outward at changing contexts and communicating with external stakeholders, competitors and customers.

Manage Effects, Not Triggers: We have to be careful not to confuse cause and effect. Humans can go three minutes without air, three days without water and three weeks without food. We need to think about critical dependencies and how long we can go without them, independent of causes. That creates the framework for prioritizing risks and allocating resources.

Prior to September 2005, the secretary of the Department of Homeland Security would have said that the primary risk he was responsible for was terrorism. Post-Katrina, the thinking about risk and risk triage changed completely. Katrina was a weapon of mass effect. We cannot completely remove the prevention framework, but to manage bigger risks, you need to manage outcomes and effects, not just triggers.

Implement Resilience: The C-suite and the board need to buy into resilience. If the tone at the top is not there, resilience will not be pervasive across the organization. Resilient organizations have three requisites: a culture of resilience, a set of business processes and enabling technologies. There need to be cross-functional teams to help implement these requisites, but accountability for resilience must reside with the people who will implement the processes.

Limits of Risk Registers: The vast majority of risk management is focused on identifying and cataloging risks. That is like keeping an accurate inventory of deck chairs on the Titanic. It is not the data that is important so much as the line of questioning—which triggers thinking rather than robotic, check-the-box responses. Risk management needs to be built into the way the business is run—one size fits one. You can "over-risk" yourself. Once you capture too many risks,

people can be paralyzed into inaction. Let's cut out 90 percent of the list and focus on the top five risks within units.

Managing Across Silos: Companies tend to manage risk well within silos, but most risk failures emerge from the white spaces between silos. One participant asked: How many people have been bitten by an elephant? Less than 10 people worldwide have died from an elephant bite. How many people have been bitten by a mosquito? At least 130 million have died from mosquito-born diseases. Within their silos, companies tend to focus on elephants. But, most organizational failures come from the mosquitoes—the little annoying things that can come back to bite us.

Where Risks Must Be Managed: Managing risk is like conducting an orchestra. The individual components are competent, but run and are synthesized by the conductor. One of the key decision points is at what level risks should be managed. There are a dozen or so risks that could bring a global corporation to its knees. All other risks are pushed down to the market levels, and managers are empowered to identify and manage the risks and opportunities they present.

Need for Offense: One can dig the deepest bunkers and pour as much concrete as possible, but someone will eventually find their way in or out of it. Unless someone is willing to play offense, organizations cannot be viewed as being resilient. It is about training an organization so that when under pressure, a framework has been established to allow the organization to consolidate its resources and lay the groundwork to emerge stronger than before. If you add just a little offensive capacity, the bad guys go elsewhere. You become an unappetizing target.

Erik Peterson, Center for Strategic and International Studies.

Seven Revolutions that Are Shaping the Future

Erik Peterson
Executive Director, Global Strategy Institute
Center for Strategic and International Studies

We are now navigating in a period of acute volatility—not just financial volatility, but critical inflection points where we see simultaneous uncertainties. We begin with a question: What will the world look like long range?

I've identified seven revolutions—each will shape our collective future and the nature of risk. They are:

- Demographic and population dynamics;
- Strategic resource management;
- Technological innovation and diffusion;
- Massive movement of data and information;
- Global economic integration;
- Conflict; and
- Challenge of governance.

Demographics: What will be the shape of the human family? There were 150 million humans at time of Julius Caesar. By 2025, the population is projected to rise to 8 billion; 8.8 billion by 2040 and 9.2 billion by mid-century.

In the developed world, we will face an aging population. We are reaching a critical tipping point where there will be more older people than younger people—a narrowing base of support for an aging population. High rates of population growth will occur in the emerging economies least able to support it. This suggests that we may want to be alert to the potential for significant migration patterns, economic as well as climate migrants.

Resources: How will the planet—food, water and energy—support this population base? Shortages of water will be a key constraint. If we could compress all the water on the planet into a single gallon, four ounces would be fresh water. Of those four ounces, two drops would be accessible to humanity, of which one drop is already in use. There are 880 milion people who lack ready access to clean water—in precisely the regions with high population growth.

Technology Revolution: The accelerating pace of technology change is a third revolution. It has been a "fasten your seat belt" ride in both deep computing as well as pervasive computing. Consider that the latest generation of supercomputer—the petaflop computer—can perform 154,000 calculations per second for every human on the planet. In computing, robotics, biotechnologies and nanotechnologies, the pace of change is accelerating, creating risk and opportunities simultaneously.

Information Revolution: The access to and rapidity of information flow is fundamentally changing the career paths and competition. The Department of Labor suggests that workers will go through 10 to 14 jobs before they reach their mid-thirties and continuously re-learn and re-tool. Tom Friedman identified the practical implications of the rapid and seamless flow of information. Thirty-five years ago, there was no question that it was better to be a B student in Bethesda than a genius in Bangalore. Today, with global and open information networks, you can innovate without having to emigrate.

Global Economic Integration: We have arrived at a unique moment, as Henry Kissinger has argued: A genuinely global economic system has come into being with prospects of heretofore unimaginable well being—but, at the same time, this system has brought about a process of nationalism that threatens its very fulfillment. We are watching a fundamental shift in the global distribution of production as well as consumption, representing a reshuffling of the global economic order. The IMF noted that the GDPs of four emerging economies—China, India, Brazil and Russia—will overtake the G-6 by 2040. Eighty percent of middle income consumers will be outside the developed world.

Conflict: We need to be thinking about scenarios in which terrorist groups use 9/11 as a baseline for success. Sam Nunn argues that nuclear and radiological threats are on the horizon. Biological threats cannot be far behind. Indeed, we had two anthrax incidents in Washington, D.C., which were expensive to clean up and potentially just a down payment on what could happen with more advanced pathogens. This means that we need to be thinking in terms of a higher probability of superviolent attacks and how resilient we can make ourselves.

Governance: The final revolution is the capacity to organize to meet the challenges that lie ahead. The point of departure is that we are beyond a simple nation-state model. Corporations and NGOs have had remarkable impacts as well. Of the top 50 economic entities, nine are companies. Governments across the world, big and small, need to find a way to bridge the gap between the sophistication and complexity of the global economy and the parochial political thinking of the nation state. Unless and until new paradigms are put into place, governments run the risk of continued atomization of authority, continued dispersion of legitimacy and fragmentation of areas of interest and operation.

What makes this operating environment more challenging is the scope and scale of the risks and opportunities—hyper-promise alongside hyper-peril. The first requirement is the need for hyper-leadership with a capacity to respond. That kind of leadership is in short supply. Across governments, NGOs, private companies and even research institutes, leaders are devolving into mere managers; strategic thinking is falling prey to tactical considerations; innovation is hamstrung by rigidities; long-term planning is replaced by triage reactions; expediency is overwhelming principles; vision is painted by the numbers; and proactive strategies are yielding to reactive. We need much better leadership with a capacity to adapt aggressively to a rapidly changing environment.

Workshop Summary

Numbers Matter: Metrics for Resilience

If companies manage only what they can measure, what measures would create insights on whether organizations are resilient or not? What resiliency metrics would be meaningful to management tied to performance and risk objectives? Are measurement systems able to capture systemic risks that flow from interdependencies and externalities—risks that that individual risk functions may not capture? What metrics could communicate risk intelligence and resilience to the board, C-suite or externally?

Dashboards for Risk and Resilience

Brian Ballou and Dan Heitger
Co-Directors, Center for Business Excellence
Miami University

Dashboard are in their infancy. There is no one size fits all. Typically, it is not a question of whether metrics are available, but what are the right measures to use? How to filter out volumes of information that are available? How much internal and external data to gather and put into dashboards? Most companies focus internally to control risks, but lack a control tower to pick up external signals in the environment and bring them back into the risk management system.

Some key questions and challenges companies ought to be asking:

1 What metrics are used to report risk intelligence and resilience to the board, the C-suite or externally? Have they distinguished between emerging versus existing risks? What are the expectations of external stakeholders, and what is being communicated quantitatively?

2 How do risk metrics relate to overall performance goals—cash flow, earnings per share or other performance measurement goals? How are those metrics placed in context—how are competitors bench-marked? How are risk metrics linked to compensation?

3 Is information consistent across risk functions? Are there common denominators for making strategic decisions and conveying risk information? In some companies, each risk ends in a different non-financial metric. Others pick a financial metric to showcase how well they are meeting goals. Is there a common metric to compare across risk silos? Are there measures for business process risks that identify how risks affect the whole organization?

4 Can leading versus lagging indicators be identified? Most variables are lagging—and risk management systems have been stalled in finding the correlations and interconnections. Are there risk models that can identify problems on the horizon? Can these measures be financial?

Brian Ballou and Dan Heitger, Center for Business Excellence at Miami University

Spiros Dimolitsas, Georgetown University

Three questions executives should ask about their risk models:

- Is it right? Have the assumptions been challenged?
- How robust is it and has it been stress tested?
- How has the model changed? Indicators do not hold up for very long.

5 Are there qualitative ways of reporting risks? Is the top ten reporting list that many companies use even a good idea? Perhaps the top two risks are so big that they should just focus on those. If resilience is a process, not a specific risk, should qualitative metrics be used to describe the process? To what extent should a dashboard focus on compliance processes or risk response plans?

Communicating Risk to the Board

Spiros Dimolitsas
Senior Vice President and Chief Administrative Officer
Georgetown University

A university has an unusual risk profile in that its factors of production, production capacity and customers are all in the same place, which makes it very difficult to diversify risks.

The board has expressed an interest in looking at risks more broadly, and we have provided them a dashboard to prioritize by type of risk and impact of risk. It characterizes risks in two ways, by "type" and by "impact."

Types of Risk

- Community risks—things that can harm people or infrastructure
- Business continuity risks—failure of systems to perform as designed
- Business performance risks— failure of systems to perform as needed
- Financing risks—things that can deplete the cash needed to run operations

Impact of Risk

Each type of risk is grouped by likelihood and threshold of impact (medium, high, low, severe). For example, a severe community risk might be a death on campus. Disruption of a major revenue line by more than four weeks would be a severe business continuity risk. Reputational risks, such as a drop in national ranking or in the competitiveness of the student body, would constitute a severe business performance risk.

Resilience Metrics

We have also developed a framework to report how resilient we are. Bad things have two dimensions: how long they last and how widespread. If you think about extent and duration, you can construct a two-by-two table: localized short term and localized long term, and widespread short term and wide-spread long term. A less resilient system would only be able to handle a short term, localized disruption. A more resilient system should be able to handle a longer term, more widespread disruption.

Tom O'Neil, Sandler O'Neil

Larry Rittenberg, University of Wisconsin, Madison; COSO

Mark Layton, Deloitte

Ambassador Roy Ferguson, New Zealand

Views From the C-Suite

A Dialogue among Tom O'Neil, managing partner of Sandler O'Neil; Larry Rittenberg, professor of accounting and information systems at the University of Wisconsin, Madison, and chair of COSO; Mark Layton, Managing Director Deloitte; Ambassador Roy Ferguson, New Zealand Ambassador; and Charles O. Holliday, Jr., CEO of DuPont. Moderated by Deborah L. Wince Smith, president and CEO of the Council on Competitiveness.

Wince Smith: How can we strengthen the ability of boards to deal with enterprise risk and resilience?

Rittenberg: There are several key things boards can do to strengthen their risk management capabilities and competencies. First, boards need to understand that risk management is a process, not a project. Second, they need to ensure that the level of risk appetite is understood and articulated and that there is a big red button that goes off every time the organization assumes risks beyond its risk appetite. Third, they need to understand the economic risks facing the company and how well they're being monitored on an ongoing basis. In most cases, this is done well but there is often not the same level of due diligence applied to mergers and acquisitions as there is to internal investments. Fourth, boards need to ensure that they understand the totality of risks the company faces. And finally, boards need to understand that the risk mitigation plans that management has put in place are working.

O'Neil: At ADM, the board has made risk management—in all its permutations from reputational risk to event risk—part of the compensation package. That affects a fairly large pool of highly paid executives. If risk management starts at the top, if it is part of the compensation package, if management embraces it and it's part of the corporate DNA, companies will get through crises.

Wince Smith: DuPont has been a global leader in integrated safety. How can we do the same with enterprise resilience—make it cultural and viral?

Holliday: A key to organizational resilience is to tell the stories that reinforce core values and culture. If we get into a crisis situation, we go back to these core values This company is 206 years old. When our founder created the company, he set a standard that has created a culture of safety. He built his home above the black powder mill. His home was the closest to the mill. If there was an explosion, he was going to feel it first. That sent a powerful message about caring about safety and caring about our people. Anytime there was a new formulation of powder, a family member of his was present at the testing of the process. If it wasn't safe enough for a family member, it wasn't safe enough for an employee.

These are the stories that have been told over and over again throughout DuPont's history. Every organization has stories that reinforce core values in the

Charles O. Holliday, Jr., DuPont

Deborah L. Wince Smith, Council on Competitiveness

telling and retelling. And, the stories are so powerful that they carry the values wherever the company does business.

Wince Smith: We don't typically think of governments being at the forefront of risk management. Can you tell us what New Zealand is doing in this area?

Ferguson: Risk management really started to enter government circles 8-9 years ago. At the simplest level, it was about natural disasters and rescuing our citizens. But, eventually risk management has been built into our planning and accountability processes. The objective has been to get every manager thinking about risks and mitigation. Every government department produces a statement of intent—like a corporate plan—that sets out major objectives and outputs. Each plan is required to identify risks, risk mitigation strategies, and key measures of success. For example, at the Foreign Ministry, one of our risks is strategic leadership. The challenge in the policy areas are sometimes even greater than for business. For example, a free-trade agreement is one of the goals, but the increasing protectionism in Congress is a strategic risk—one that we're not sure how to mitigate.

Wince Smith: Audit committees have been double or triple-purposing—serving as a proxy for a risk committee. If a separate risk committee is created, how do we make sure that the full board has a meaningful role in risk oversight?

Layton: Too frequently, the audit committees focused on compliance, losing the broader focus of risk. Even if separate committees were created, they would need to be aligned. But, the right structure might be different for Fortune 100 and 1000 companies, given the differences in scalability and competencies.

Rittenberg: Risk and strategy are totally intertwined, so there has to be a risk discussion at the full board level. It can't be put off as a compliance issue. Resilience goes one step beyond risk management. When we talk about risk we talk about probabilities. But, resilience means that if worst case scenarios actually occur, you may still be in a position to survive and take advantage.

O'Neil: The entire board is responsible for risk. It can't be in a stovepiped committee. You can't report out on it. Full responsibility should rest with the CEO. Collectively as a board, if there's any doubt that senior management does not fully embrace it, they should be out in five months instead of five years. Things move too quickly. Information moves fast. What would appear to be a minor incident becomes a major ecological disaster because two gallons of something ended up in the river. One thing I do as chairman of the ADM audit committee is go out to dinner the night before a board meeting with as many of the staff of internal audit as I can. I told them I only want to hear the bad news, not the good news. I've encouraged the other board members to do the same in their areas of oversight.

Pat Gnazzo, CA Inc.

John O'Connor, Cisco

Leading Indicators

Leading indicators are difficult to identify. Sometimes it is not whether you can predict the indicator, but whether you can rapidly assess how it will impact your position. As a service organization, one of our concerns is the volatility and rising levels of benefits packages. The benefits budget is significant—20 percent of operational budget. We might not be able to predict everything that could impact the cost of benefits, for example, a change in the social security floor, but we have developed a methodology to assess how quickly a change would be digested through the system and what it would do to our cash position.

Managing and Mitigating Risk

Pat Gnazzo
Senior Vice President, U.S. Public Sector Business
CA Inc.

Compliance, risk and business continuity are all intertwined. A couple of cautions. We need to be careful about using someone else's template. One size does not fit all. Every company is different. Every university is different. Risks are different across sectors and universities. Risks have to be understood within the context of a specific business.

Companies have been assessing risk for years, but they do not put it in a form that boards can use. The problem is the lack of a good tool that allows information to bubble up to senior management. Every organization should understand its risk appetite and its risks.

That plan needs to reach down to the business units—their operating plans should talk about the risks of not meeting goals and the actions it will take to mitigate those risks. Risk management has to start at the bottom. You cannot understand it from an enterprise basis if you do not understand it at the business unit level. For example, everyone has a budget. What are the risks of changes to the budget, and how will the business units mitigate that risk?

The top ten enterprise risks are important, but we cannot forget that every department within an organization should have a top ten risk list as well. If each one of those departments is not working on its top ten risks, the company is exposed. We may be handling the Katrina and bird flu risks, but we are missing the department risks. There will always be a top ten, because when you mitigate some risks other will emerge. That is what managing risk is all about.

Resilience Metrics: Time to Recovery

John O'Connor
Director of Supply Chain Risk Management
Cisco

My perspective is functionally oriented toward supply chain risks. Cisco has an enterprise risk management group focused on assessment and identification of top risks. They coordinate activity, but the functions drive the risk intelligence and resiliency programs.

What can we measure, and what should we measure? Cisco has identified a key quantitative metric: time to recovery. Our business continuity program (BCP) assesses our strategic nodes—core suppli-

ers, transportation hubs, logistics nodes, manufacturing nodes—and asks: Regardless of disruption, what is the time to recovery for each of these nodes? Regardless of the disruption, how long does it take us to go from a catastrophic disruption with zero output back to 100 percent? That is our measure of resilience: TTR or time to recovery.

We spent a lot of time on that information set because understanding recovery time is a key piece of information for crisis management. Whether it is a Chengdu earthquake or a Hurricane Ike, we understand where nodes in that region are and how long it takes for them to recover. We can assess the impact immediately. This informs not only our crisis management but also our resiliency programs. We understand where we have exposures and where we need to allocate resources to drive recovery. BCP may come off as a dry process, but it is a key enabler.

We have BCP coverage as a metric and response rates as a requirement, and we measure our suppliers against that.

We pair risk intelligence—knowing where our vulnerabilities are—with risk analytics. We have collected large series of data sets—historic food data, incident data, simulation analysis—which tell us where we have the greatest probabilities of disruption.

This allows us to look at operational risks and natural disasters as one set. It tells us where we are more likely to experience a disruption. That is all interesting and informative, but the data has not been terribly operational. Risk programs are not generally tailored to risk analytics for a couple of reasons. You are always going to pick the wrong risk.

At the end of the day, we found that revenue is the key attribute that focuses risk programs. Obviously we have a program that takes care of our people first, but a risk focus on revenue allows us to look after both our shareholders and customers. Cisco is unique in that it has 200 product families and 8,500 products. But 100 products account for 50 percent of revenue, so it is a relatively easy answer about where to focus.

How do you determine your risk appetite? That is an interesting question, but the simple answer is that risk appetite will never match risk budget. For $100 million, we could de-risk the entire supply chain. Although we have a great budget, it is no where near enough to guarantee a risk-free supply chain. When setting our risk budget, we also think about the impact on gross margin and on external insurance. So, risk appetite needs to be anchored in something far more tangible.

We have been talking about risk intelligence—gathering information, understanding vulnerabilities and making sure you have playbooks and processes—but we have not really discussed resilience. Whatever vulnerabilities we identify, they are still going to be there. This to me is the difference between risk intelligence and resilience. For Cisco, resilience is about recovery time goals for each of the nodes—and that recovery time may or may not be acceptable. If the node is something with a simple process, like pack-

aging material, they can recover in a week. So we can check the box and move on. But, if it is a manufacturing node, recovery time following a disruption could take months, with serious repercussions for our customers and shareholders. So we set goals for our manufacturing nodes, our component suppliers and our transportation hubs, and then work our resilience program to bring the recovery time in line with our goals. It is about focusing our on our recovery time for key products and nodes.

The one thing that we are finding is that effective crisis management is usually a function of budget and time; every company needs to have the ability to identify and respond. There is not a budget excuse for not having those capabilities.

Key Observations from the Discussions

Culture Is Key: Without leadership commitment, resilience is just an exercise.

Metrics for the Board: Communicating the right metrics to the board is the Holy Grail. But, there are some key questions. Finding the right balance between high-level and simplified, and creating a few data points that are both insightful and impactful, is hard. Core business metrics have to be filtered; "need-to-know" is an important way of thinking about that filter. Some metrics can be standardized and repeated. Others wax and wane in importance.

There is a danger in having too many dials on the risk dashboard. Communications should be simple and focused on the critical operating tasks for your organization. We are enabling data, but we are lagging in developing the tools to understand what it means.

For risk management to have value, the metrics cannot be just defensive. We need to think about it as an enabler of value creation. Effective risk management enables companies to be up and running while competitors are paralyzed. Resilient entities have a competitive edge.

The information that the board gets is focused on risk minimization and control. But, how do we communicate resilience? Boards may become complacent that their risks are under control, but they are not getting the metrics that would indicate whether the company has the ability to anticipate risks or the processes to recover.

The risk factors that we tell investors and analysts are not the same as the ones reported to the board. The disclosures in an SEC quarterly filing are known risks. What bubbles up to the board are things that you would never want to put in public documents—for example, that a competitor has come out with a much better product.

Value of Metrics: Is normalization of numbers even valuable? Risk professionals spend hours trying to come up with scoring methodologies that create comparability, but in reality they are comparing apples and bananas. In our zeal to create comparability, we may have moved away from an understanding of what the risks actually are.

We created tools to enable common understandings about risk. We took compliance, SOX, internal audit and operational risk, and standardized the risk categories and definitions for all control functions across a four-by-four grid of critical, high, moderate and low. The key point was that we standardized what "critical" meant for each of the businesses. So, when the audit said that something in retail was critical, they were using the same probability and impact framework as all the other businesses. That has helped with comparisons at the strategic level.

That makes the board conversation a little more understandable. Frankly, what we heard from the board members is that they do not want over-scientification of this risk information. Too many things have numbers on them; inventing a number is not data and it does not necessarily provide risk insight.

No process should replace judgment. We need to present quantitative numbers, but the story that goes around them will be determined by our objectives and risk appetite. Our job should be to put those metrics in a context that the board can understand—something like a stoplight approach, which is a way to convert quantitative information into qualitative. It translates numbers into a bright line threshold that tells them they need to be concerned.

Data is nothing more than a series of numbers. Once it becomes meaningful, it is information. But, it does not turn into knowledge until you absorb it, process it and do something about it. The evolution is data, information, knowledge. Whatever metrics are used, they need to represent the language of business (ROI, IRR), not the more specialized language of specific functions.

Frequency of Risk Reporting: Frequency of reporting is determined very much by risk volatility. There are some risks that are stable over time, so they will be reported on a quarterly basis. Others are so volatile that they need to be discussed more frequently. There is a big difference between a crisis and a non-crisis environment in reporting frequency.

Two seconds of lost time can be a potential disaster. The issue is whether the board has defined a critical time frame, not how often is risk reported.

Leading Versus Lagging Metrics

- Looking for leading indicators in vast data sets is probably a needle in a haystack scenario. But, those data sets are good for anomaly detection—specifically where variables are changing at a rate that is outside their normal patterns.
- Human Resource is another good predictive indicator. The reason employee problems emerge is highly indicative of potential risks. Questions that might be asked include: Do employees engage in additional training which indicates satisfaction? Do they pursue certain groups or managers? Is there a training readiness regime that follows incidents?
- Near misses create a good learning opportunity to illuminate a risk area or vulnerability and close the gap.
- A framework that can help model and anticipate risk is: "Change happens around you. Change happens to you. And change happens because of you."
- Lagging indicators should be fed back into risk models to improve predictive capabilities.

Too Good To Be True: Risks metrics should also tell you when something is too good to be true. Good news should be challenged just as much as bad news. The board should be questioning good results as well as poor ones.

Value of Cross-Functional Teams in Risk Management: My company has historically been very careful about its internet protocol and trade secrets, but as we moved from the paper to the digital world, some of that discipline faded. Two years ago, one research scientist pled guilty to economic espionage. The CEO wanted to know what controls we would put in place today if the problem were being dealt with five years hence. That led to the creation of a cross-functional team that includes business units, with every function in the company doing a very in-depth analysis of failure modes. We now have a trade secret risk management in every business, every function and every region. It is understood where our crown jewels and critical assets are and how well protected they are. As a result of this one event—which could have been treated as a one-off—cross functional teams, process owners, metrics and solutions for a range of potential problems in this area were created.

Charles O. Holliday, Jr., DuPont

Coping with Crisis, DuPont Style

Charles O. Holliday, Jr.
CEO DuPont

We have learned a couple of key lessons.

- First, you can never anticipate the crisis you get.
- Second, if your systems are resilient enough, you can manage pretty much anything that comes up
- Third, raise the warning flags early. People are often reluctant to call a crisis. A few examples:

Case 1: Crisis or Not?

One Wednesday at 5:00, when I was head of DuPont's Asia Pacific business based in Tokyo, I received a call from a person who said he was the Swiss ambassador. He said a DuPont employee had broken into the embassy and threatened to kill him. This was potentially an international incident on sovereign Swiss soil involving the Swiss, Japanese and U.S. governments with DuPont at fault.

Here is the rest of the story: The employee lived four houses away from the embassy. His wife was pregnant and due very soon. He had complained multiple times that the embassy guests were blocking his driveway so he could not get out in the event that his wife went into labor. And he could not call emergency services because he did not speak Japanese. And, although he got angry enough to issue threats, he was not actually armed. We did not call the U.S. embassy or Wilmington. We decided to work it through. And, two days later, the ambassador invited the employee and his wife for dinner and an apology.

All the trappings, but no crisis.

Case 2: Crisis or Not?

The scene is Northern India. DuPont had a contract to sell technology to a plant under construction. At 2:00 a.m., rebels went in an pulled five people out of their dorms and assassinated them. DuPont had no one on site.

Most thought it was a terrible tragedy. Few would have seen a crisis coming. But the next morning, the factory owner gave an interview to the news media and said that DuPont caused the deaths. His logic was that DuPont had advised them to keep the guns locked up since the vessels that were being delivered would not have reacted well to a gunshot. The next morning the parliament of India was debating what charges should be brought against DuPont.

Crisis or Not? We did react very seriously. We got the right information out to the public, talked to the owner and got him to retract his statement, and shut the crisis down in 24 hours. Because of how the media handled it, what would have been a terrible tragedy in any event turned into a crisis. So the message is that the organization will tend not to call a crisis.

Crisis Management at DuPont: The key to managing crisis is to create a resilient crisis management process and pressure test it.

At DuPont, there are 17 crisis management teams. The leaders of each of those teams are continually on alert and empowered to call a crisis. The first question that is asked is whether it should be a corporate crisis. Those actually have not been called very often—9/11 was the first.

The leaders of the 17 groups can be rallied to a central crisis management room in 30 minutes—and we find that the room itself creates its own kind of focus and mindset.

The CEO has specific crisis communications roles—with the media, the government, suppliers, families. Given those responsibilities, the DuPont CEO does not manage the crisis teams.

Because people tend not to take crisis tests very seriously, we have stretched the definition of crisis to include important events, but maybe not the traditional definition of crisis events. On a Friday afternoon about a year ago, I was in New York meeting with customers when my blackberry started to do its shaking thing. I looked down and read: "No crisis, call immediately." Within a few minutes, I learned that President Bush was planning a visit—the next Tuesday—and the secret service and advance people were already on their way. As we were thinking about how to get ready for that visit, we decided to activate our corporate crisis process—and it worked brilliantly. We were able to rally everyone in the company virtually overnight.

Strategic Resilience at DuPont: Back in late 1980s, Greenpeace scaled the fence on a cold rainy day and hung a big banner from the top of the water tower that said: "DuPont, No. 1 polluter." The word "polluter" was so low that it was below the fence line. So all the people outside could see was: "DuPont, No. 1." Most people thought we had won another award. Our plant manager handled the Greenpeace guys, got them down safely, and we were dealt with pretty gently on the evening news. So, we were sitting around the next day, patting ourselves on the back, and one lone voice said: "But they're right." He said that we put out more stuff than anyone else. You could have heard a pin drop. And everyone was thinking: "Who is this soon to be unemployed person?"

But, for me, it was a watershed moment. We might be the biggest, but we spent the next decade trying to fix our processes to reduce our footprint. As a result of that work, we have reduced our greenhouse gas emissions by 72 percent while we increased our volume by 40 percent, and we got good returns for our shareholders every time.

Workshop Summary

Actions Matter: Incentives for Resilience

At the end of the day, companies need to create a system that drives toward resilience. What role can market movers play in helping to move organizations toward more effective risk management and resilience? What can government do to reinforce private sector drivers and market mechanisms that encourage/reward resilience processes? How should the public and private sectors be working together to create a more resilient country?

The Role of Audit

Christine St. Clare
Audit Partner
KPMG

The audit profession is risk averse, so it is hard to imagine rapid innovation in risk reporting in non-financial areas. However, the fastest inroads are being made in the areas of sustainability and corporate social responsibility (CSR) reporting. Increasingly, senior management sees non-financial reporting as a crucial companion to financial reporting.

Today, the real question is not who is doing CSR reporting, but who is not. Every three years, KPMG conducts a global study. We found significant increases in the number of companies reporting. CSR has become a more mainstream practice around the world—and the U.S. is lagging. We are near the bottom of 22 countries.

For the Global 250, more than half are linking their reports to metrics. This is driving a need for more non-financial data that is credible and can stand up to scrutiny. Until recently, there has been criticism around self-serving reports that were generated by external PR offices.

Historically, financial reporting was directed to shareholders. The evolution now is toward CSR reporting directed to a broader audience of stakeholders. Today, stakeholders are asking that reporting be linked to strategy, risk, business processes, governance and concrete performance indicators or metrics.

Since sustainability reporting is voluntary, guidelines have been slower to emerge. The guidelines commonly used are published by the Global Reporting Initiative. These guidelines created a more data-driven, structured way of reporting that creates comparability. That is what is needed for the accounting industry to have a credible assurance or attestation capability.

We could take an hour and not exhaust the list of stakeholders who want more reporting and more transparency in CSR reports. To name just a few, the Carbon Disclosure Project, a collaboration of 300 institutional investors, is calling better disclosure around risk to be included in 10K filings. The Coalition of Environmentally Responsible Economies petitioned the SEC to force registrants to disclose financial risk and opportunities around climate change. The Climate Action Partnership's lobbying effort for federal regulations on greenhouse gas emission (to forestall a patchwork quilt of state regulations) could drive more reporting requirements. The

Christine St. Clare, KPMG

Linda Conrad, Zurich

Grocery Manufacturers of America are working with their members to measure carbon footprints from production to consumption.

The Dow Jones Sustainability Index is ranking performance related to environmental programs. Walmart recently brought together its suppliers with NGOs and Chinese officials to discuss how to bring sustainability and risk mitigation into the supply chain.

All of this creates pressures to collect data that can be verified by the audit community.

In the sustainability area, the United States lags in developing approaches and standards that can be attested to. And, basic requirements for attestation are missing in the risk reporting area, including lack of a common language of risk, lack of standard taxonomy even within an organization, and one size fits one approaches which are at odds with the uniformity of reporting approach requirements. Moreover, auditors will have difficulty with the issue of emerging versus existing risk.

The opportunity to get more uniformity and acceptance of risk reporting and performance indicators is there, but much more groundwork must be laid. If the other stakeholders keep up the pressure for more reporting, as they have done in CSR and sustainability, the accounting profession will continue to move into the area of non-financial risk attestation.

The Role of Insurance

Linda Conrad
Director Risk Engineering, North America
Zurich

Insurance is in the business of risk. It is what we do for a living. Our motto is: "change happens." Last year we delineated that into three sections: Change happens around you (that you cannot necessarily control); change happens to you and change happens because of you. That helps you delineate those things over which you do have control versus the things you do not control but to which you must be prepared to respond.

Many people think of insurance as lines of business; as discrete risk solutions for certain problems. But I think we do ourselves as an industry a disservice if we do not look beyond insured risks. No company would look at its exposure just in terms of property risk. We need to look at the entire risk that companies face, not just their insurable risk. Insurance is only a small piece, maybe 20 percent to 40 percent, of a company's risk picture. If we only look at the insured portion, we are not working as a partner.

A case in point. We conducted a risk profiling session with a food additive company. Someone in accounting stood up and said that they had a fantastic new sales partner which represented some 25 percent to 30 percent of business. The new sales partner was an aviation company buying up food additives for de-icing purposes. We were insuring them for product liability—but this use was not part of the coverage.

Phil Auerswald, George Mason University

We are not working well with our customers if we do not help them look at things that could come out of nowhere.

Most people tend to think of insurance as set it and forget it. If structured correctly, they think that once the insurance coverage is in place, they can move on. But risk is dynamic and needs to be revisited often. If we are not constantly re-evaluating, we are not adequately covering even the insured risks, let alone the risks that are uninsurable, like reputation and brand.

Insurance needs to get out of the old century and become more like a GPS system. Risk intelligence is GPS. If you are going down a path and miss the turn, your strategic decisions need to realign. Even more importantly, you have to keep checking whether you are headed toward the right address.

The Role of Public Policy

Phil Auerswald
Professor of Public Policy
George Mason University

When we think about responsibilities, risks and events, there is scalability. Low impact events are usually managed by individuals or by operations people in a company. Larger-scale events might be the responsibility of a CEO or a mayor. And then there are problems that are much larger—and go beyond the fence line or the municipal boundary. These situations are too large for any one company or jurisdiction to handle, even if their survival is threatened. Those will be the challenges that the government has to lead.

Although its focus is often on high-impact, low-probability events, the government has an interest in understanding risk across the board—just as companies have an interest in understanding risk that goes outside their firms. So there is a convergence of questions being asked, decisions being made and, surprisingly, even of objectives. All of this could have the fortuitous effect of creating an era of better and different government, and better and different business. But, there are no guarantees it will happen that way.

The 2008-2009 global financial crisis could inform a whole new vision of how the government should partner with business. But, that is not where we are headed. On one hand, the central take-away of the discussion is that government was not paying attention and did not perform its regulatory functions. On the other hand, it is that businesses were greedy and did not care about the soundness of the financial system.

This crisis should have stimulated a conversation about opportunities for public and private mission sharing. This will have to be an activity in which both sides leave behind the 20th century. The private sector has to be leave behind the old adages of "don't regulate us, we know what we're doing;" "the free market can solve its own problems;" and "resources will be allocated when we let the market determine what will function best." For its part, the government must understand that more compliance directives, more regulation and more standards of different types do not make good use of the capabilities of

the 21st century. We have got to use the technology, build the trust and tap into the tremendous knowledge bases at companies like Deloitte, Walmart and DuPont to think about risk solutions. And then we need to put into place policy approaches that have the potential to use the market and business intelligence in service of the country and the rest of the world.

Key Observations from the Discussions

The question was asked whether it should be the job of auditors to ensure that a risk tolerance level has been set and that risk processes are being followed.

One view was that the profession's main focus is to improve the quality of the financial statement audit and to provide an assurance on the financial results of the company. When management and governance gets involved with the identification of risk and puts the data collection systems in place, it makes us better auditors. But, that is different than asking auditors to report on risks tied to external factors—environment, social and climate change risks articulated in a CSR report. It took centuries to get to the current standards around auditing financial statements. We are going to have to move more quickly—the world and stakeholders are demanding it.

Another agreed that the audit community could do much more. When we look at what the profession does when it comes to financial statements, there is probably only one item in the financial statements that the accountant opines on, which is not even disclosed in most cases. That is the "going concern" opinion. Everything else is historical data, looking backward, which we attest to. But management provides much more information in the discussion and analysis section of the annual report. And there is even more disclosure in the risk sections of the SEC 10K reports. But the auditors have no responsibility to review them. We are reaching a convergence point where we all have to work together as a community—public policy, insurers, auditors—to have better disclosures. We are all feeling the pressure of the credit crisis—where were the auditors, where were the risk managers, where were the regulators, where were the CEOs? Let's move out of where we were—out of centuries of standard practices—to move the ball along.

Following the workshop, Phil Auerswald and Debra van Opstal examined some specific ways that public policy could reinforce market incentives for resilience in the article, "Coping with Turbulence: The Resilience Imperative" in the journal *Innovations* (Davos Edition, January 2009). They wrote:

"Since the data show that the companies that are more risk intelligent and resilient actually do better in the market, the question might well be asked: Why doesn't the market reward these qualities with better ratings and lower insurance premiums?

And what can the public sector do to reinforce market mechanisms?

The ratings agencies and insurers are already moving in this direction. Standard & Poor's, for example, is carefully integrating enterprise risk management into its ratings assessment. And some of the leading insurers and re-insurers are creating market incentives to encourage their adoption.

Adopt New Disclosure Requirements. The government could reinforce these trends through more targeted disclosure of non-financial and strategic risks to the Securities and Exchange Commission (SEC). It could also require companies to disclose more about their risk-management processes.

We can look back a decade to see how this might work. The year was 1998 and Y2K concerns were sweeping the globe. The SEC chairman, Arthur Levitt, sent this statement to more than 9,000 publicly traded firms:

"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 feel that this programming flaw could debilitate computer systems worldwide….Time is short. Because the lack of information regarding your preparations for the year 2000 could seriously undermine the confidence that investors place in your company, it is imperative that you provide thorough, meaningful disclosure on this topic."[1]

In the Y2K case, the government asked the companies to expose not their vulnerabilities but their readiness to deal with risk. Today, the capacity to manage risk and to rebound from disruption is increasingly relevant to earnings and shareholder value.

Companies may not be able to project a specific probability of risk for all contingencies. But they can certainly disclose more about their risk management practices, the composition of their risk committees (which traditionally has been limited to credit and market risk specialists), and their oversight by the governance system. Understanding a company's readiness to deal with risk and capacity to respond to disruption is likely to become extremely relevant as a predictor of future earnings—and extremely useful in creating incentives that make societies more resilient.

Incorporate Risk Engineering Principles. Public policies for insurance coverage that ignore the relationship between level of risk and risk pricing have been less than effective—and may actually reduce expenditures for preparedness and prevention.[2]

In contrast, some of the leading insurers and reinsurers are developing robust principles and best practices for risk engineering and resilience and rewarding clients that adopt them.

Consider this case: Ocean Spray, with a plant on the Gulf Coast of Florida, calculated that a major hurricane could cause a $75 million to $100 million loss. Risk engineering experts advised it on how to secure sections of the buildings most vulnerable to high winds and recommended investing in backup power generators to protect its grapefruit inventory.

During the wild hurricane season of 2004, the plant took direct hits from two of the four hurricanes that struck the Florida coastline with only superficial damage and minimal losses. Indeed, the data show that risk engineering approaches yield dollar losses that are 75 percent to 85 percent lower. During Hurricane Katrina, clients of FM Global collectively invested $2.3 million to prevent losses that were estimated at $480 million. In other words, for every dollar spent on targeted preparedness measures, $208 was saved in one single major event.[3]

Government could incorporate systems approaches into public sector risk management practices as well. For example, public officials could factor in the cost of reconstruction and assistance following a major disaster. They might discover that they would save tax dollars by undertaking similar risk engineering in

1 Debra van Opstal, Transform, Council on Competitiveness, 2007, p. 41.

2 As a consequence of the debate over the government's recent intervention in financial markets, the principle of "moral hazard," on which this observation is based, has moved from textbook obscurity to global notoriety in a matter of weeks.

3 William Raisch and Matt Statler, *Crediting Preparedness*, International Center for Enterprise Preparedness, NYU, August 2, 2006. http://www.nyu.edu/intercep/research/

publicly-owned facilities and infrastructure, and offering homeowners incentives to do the same—before a disaster occurs.

Create Market Financing for Disasters. Finally, government can partner with the private sector to create innovative financing mechanisms that fund recovery from natural disasters. Floods, storms, earthquakes and heat waves place a huge burden on the public sector, which not only carries the cost of relief efforts but is also responsible for rebuilding public infrastructure.

Moreover, public entities consciously or unconsciously decide to retain risk by not insuring their infrastructure. For example, in 2005, economic losses from natural catastrophes hit a record high, with direct financial losses of $230 billion (0.5 percent of total worldwide GDP). Despite a record insurance payout of more than $83 billion, uninsured direct losses of $150 billion had to be carried by individuals, companies and the public sector. More recently, in 2007, a total of 335 natural catastrophes led to losses of $64 billion across the globe, of which $40 billion were uninsured.[4]

Traditionally, the public sector has adopted a post-event approach to disaster funding, including increasing taxes, reallocating funds from other budget items, accessing domestic and international credit, and borrowing from multilateral financial institutions. Most rely on assistance from international aid.

Pursuing a post-disaster strategy has several potential disadvantages for governments. Funds are diverted from key development projects to pay for emergency relief. Governments must pay the premium to raise new domestic debt in a credit constrained, post-event market, and raising taxes can weaken the economy further and discourage new private investments. Finally, international aid often arrives too late for immediate disaster relief.

Governments could save considerable amounts by shifting from relief to pre-event risk financing; that is, by setting up solutions that involve financial reserves, contingent debt agreements, insurance and alternative risk transfers. How could this work? One example is catastrophe bonds that transfer risks from the sponsors to market investors. In essence, the bond offers investors an attractive risk/return profile. The issuer invests the capital in low-risk securities (such as treasuries) and the interest plus a premium is paid to the investors. If the bond matures without the pre-specified event occurring, the principal is repaid to the investors, similar to regular bonds. If a catastrophe does occur that "triggers" the bond, investors may lose some or all of the investment principal they have paid. In that event, the funds are paid to the bond sponsor to cover losses.

We are now facing a new set of risk dichotomies that demand new approaches in the way countries, companies, communities and citizens prepare for and manage risk, and prepare for resilience.

In the 20th century, paradigms of security evolved from Maginot lines to doctrines of containment to firewalls. Each succumbed in its turn to technology and globalization. At the start of the 21st century, the very notion of security defined in terms of "perimeter defense" or "threat containment" has become all but obsolete.

Today's threats are too ubiquitous to be isolated and too nimble to be contained.

In such a world, responsible companies and governments are compelled to emphasize accessible actions rather than illusory remedies. In such a world, resilience is no longer an afterthought. It is an imperative.

4 *Disaster Risk Financing: Reducing the Burden on Public Budgets*. Swiss Re, June 2008.

Henry Ristuccia, Deloitte & Touche

Vikram Mahidar, Deloitte

Challenges for Corporate Risk Managers

Henry Ristuccia
Partner
Deloitte & Touche

Vikram Mahidar
Senior Research Manager
Deloitte

What we find in many companies is that risk management activity is driven by both regulation and business needs. But, the connectors are lacking—both across the organization and up the organizational ladder.

One of the most serious gaps is the disconnect between the risk management functions—where most of the heavy lifting occurs—and the senior executives and governing bodies that are ultimately responsible for risk management. There is no common definition of organizational framework for managing risk, no well understood roles and responsibilities and no way to measure or monitor effectiveness.

A few weeks ago, I asked the CEO of a financial institution—one that has fared better than its peers—how its risk management programs were related to the risks identified in the company's 10K. He said: "That's the problem; they don't." The biggest opportunities to transform risk management are in filling in the gaps between the risk management activities and senior managers. These broken links have serious implications for the bottom line: incomplete and inaccurate information, false positives as well as false negatives, and inefficient use of resources.

Many of the following nine principles of a risk-intelligent enterprise focus on a transformation at the executive level. The characteristics of risk intelligence include:

- Common definition of risk that addresses both the value preservation and the value creation sides—consistently and throughout the organization;
- Common risk framework supported by appropriate standards;
- Key roles, responsibilities and authorities clearly defined and delineated;
- Common risk management infrastructure to support business units and functions;
- Appropriate transparency and visibility into risk management processes for the board;
- Executive management charged with primary responsibility for designing, implementing and maintaining an effective risk management process;
- Business units given responsibility for management of risk within the organizational framework;
- Certain functions (finance, legal, IT, HR) provide support to business units with respect to organizational risk management processes; and
- Ongoing and objective monitoring and reporting on effectiveness of risk programs.

Survey Results: When asked how they identify and mitigate their top five risks, most company executives said they did not manage risk that way anymore. Rather, they had created a comprehensive framework for risk management that was integrated across the organization and at multiple levels. Respondents indicated that their companies understand risks specific to their industry and business model—and many have instituted a central function charged with orchestrating risk management process—and these processes have been well-received by the business units.

That is the good news. The bad news is that most respondents were not sure whether these best practices are adequate, and they did not know whether their companies are managing risk well or not.

We identified three gaps:

1 The ultimate goal of risk management remains unclear. When we asked, how do you define risk management goals, the answers were literally all over the map. Risk disclosure statements, even within the same industry, are quite disparate, indicating that there is no common understanding of what is important. Even within the same company, there are inconsistencies about what the goal of risk management processes should be.

2 Most executives reported that they do not understand the risk management expectations of major stakeholders, such as investors.

3 Given the uncertainties, companies are finding it difficult to quantify the business impact of emerging risks.

Senior management and board level involvement remains minimal. Getting the right tone and establishing clear goals and consistent processes requires engagement by senior executives. Companies have set up risk committees, but executive involvement remains relatively sparse—as do the reports from the risk committee to the executive committee. One respondent noted that the only time the CXO gets involved is when it is time sign the SEC filing. Similarly, the balance scorecards used by the boards contain very few risk measures. We need to "balance" the balance scorecard.

Currently, risk seems to be managed from different functional organizations within the company—legal, audit, security. But, frequently, there is not ownership at the executive level. And, the people who manage risk often come from a security, intelligence, compliance or legal background. What is needed are businesses skills that complement these specialty areas. Risk professionals need to be able to translate what they see into business terms.

Participants

Erica Agiewich
Business Resiliency Manager, Workplace Resources/ Global Risk Management
Cisco Systems, Inc.

Phillip Auerswald
Director, Center for Science and Technology Policy
George Mason University

Susan R. ("Bobbi") Bailey, Ph.D.
Vice President, Global Network Operations, Planning
AT&T

Brian Ballou
Co-Director, Center for Business Excellence
Farmer School of Business
Miami University of Ohio

Mark Baylis
Senior Manager
Deloitte & Touche, LLP

C. Wm. Booher, Jr.
Chief Operating Officer
Council on Competitiveness

Margaret Brooks
Vice President of Solution Sales, Governance, Risk and Compliance
CA Inc.

Judith Cardenas
Chairman and CEO,
Center for Performance and Accountability

Jane Carlin
Global Head of Operational Risk, BCP, and Information Security
Morgan Stanley

Linda Conrad
Director, Customer Enterprise Risk Management
Zurich

Kristy Coviello
Marketing Manager
Deloitte & Touche, LLP

Spiros Dimolitsas
Senior Vice President and Chief Administrative Officer
Georgetown University

Edward Donnelly
Senior Fellow
Council on Competitiveness

His Excellency Roy Ferguson
New Zealand Ambassador to the United States

Joseph Fiksel
Principal and Co-Founder
Eco-Nomics, LLC
Executive Director, Center for Resilience
The Ohio State University

Robert Flynn
Vice President, Chief of Staff, Office the of President
Travelers Insurance

Frederick Funston
Principal and National Practice Leader for Governance and Risk Oversight
Deloitte & Touche, LLP

Carl A. Gibson
Director, Risk Management Unit
Deputy Vice President (R&A), Latrobe University, Australia

Patrick J. Gnazzo
Senior Vice President, General Manager
U.S. Public Sector Business
CA Inc.

Sharon Hake
Global Marketing Leader
DuPont

Kenneth V. Handal
Executive Vice President, Global Risk and Compliance; Chief Compliance Officer; Corporate Secretary
CA Inc.

Dan L. Heitger
Co-Director, Center for Business Excellence
Farmer School of Business
Miami University of Ohio

Mary Herbst
Director of Business Resiliency, Audit and Business Risk Management
Carlson Hotels Worldwide

Charles O. Holliday, Jr.
CEO
DuPont

Kelly Johnstone
Senior Security Manager, Strategic Security
Coca Cola

Anne Gadegaard Larsen
Advisor, Corporate Responsibility
Novo Nordisk A/S

Mark Layton
Global Leader, Enterprise Risk Services and Vice Chairman, Audit
Deloitte & Touche, LLP

Vikram Mahidhar
Senior Manager, Deloitte Research
Deloitte & Touche, LLP

Scott McHugh
Vice President, Global Asset Protection and Security
Wal-Mart Stores, Inc.

Chris McIlroy
Director, Infrastructure Protection & Resiliency Division
SRA International, Inc.

Cynthia McIntyre
Senior Vice President
Council on Competitiveness

Raymond A. Mislock, Jr.
Chief Security Officer
DuPont

Robert Moore
Group VP, Global Security Group, EHS and Crisis Management
Hewlett-Packard

Darren Mulholland
Senior Vice President, Operations and Technology
NASDAQ

John O'Connor
Director of Supply Chain Risk Management
Cisco Systems, Inc.

Tom O'Neill
Principal
Sandler O'Neill & Partners, LLC

David Olive
Co-Founder
Olive, Edwards & Cooper

Erik Peterson
Senior Vice President; William A. Schreyer Chair in Global Analysis; Director, Global Strategy Institute, CSIS

Joseph Petro
Managing Director
Citigroup
Citi Security & Investigative Services (CSIS)

James Porter
Vice President and Chief Engineer—Safety, Health, & Environment and Engineering (Retired)
DuPont

William Raisch
Director, International Center for Enterprise Preparedness
New York University

Henry Ristuccia
Partner and Leader, Governance and Risk Management
Deloitte & Touche, LLP

Larry E. Rittenberg
Ernst & Young Professor of Accounting & Information Systems
University of Wisconsin
Chair, COSO

Susan Rochford
Vice President, Energy & Sustainability Initiatives
Council on Competitiveness

Steve Ross
Firm Director, Security Services
Deloitte & Touche, LLP

Kenneth Senser
Senior Vice President for Global Security, Aviation and Travel
Wal-Mart Stores, Inc.

Erica Seville
Research Fellow
University of Canterbury

Mark Sibley
Program Director, Business Resilience, Northrop Grumman Information Technology

Steve Spoonamore
Partner
GSP LLC

Christine St. Clare
Advisory Partner
KPMG LLP

Matt Statler
Associate Director, International Center for Enterprise Preparedness
New York University

David W. Stender
Associate CIO for Cybersecurity
Chief Information Security Officer
Internal Revenue Service

Branko Terzic
Senior Energy Consultant
Deloitte & Touche, LLP

Jonathan Tetzlaff
Senior Director, Crisis Management and Threat Analysis
Merck & Co., Inc.

Betsy Thurston
Vice President, Strategic Development
Council on Competitiveness

Steven Trevino
Managing Director
Resilient Civilization Initiative

Debra van Opstal
Senior Vice President
Council on Competitiveness

Deborah L. Wince-Smith
President
Council on Competitiveness

Kirsten Edmondson Wolfe
Vice President, Marketing
CA Inc.

Rob Zanella
Vice President, IT Compliance
CA Inc.

COUNCIL STAFF

David Padgham
Policy Director
Council on Competitiveness

Mildred Porter
Meeting Planner
Council on Competitiveness

Michael Ruthenberg-Marshall
Intern
Council on Competitiveness

Briefing Materials

Warning: Turbulence Ahead

Overview

Globalization, competition, technological complexity, interdependence and speed are fundamentally changing the kinds of risks and competitive challenges that companies—and countries—face. The competition is getting much better. The world is entering an age in which "we'll all be competing with everyone, from everywhere, for everything".[1]

Technological complexity and interdependence in the global economy are increasing other risks. Extended and interdependent energy, transportation, information and communications networks can quickly magnify the impact of point failures—whether triggered by attack or accident. Operational risks, once thought to be a back office concern and trivial in comparison to market and credit risks, are becoming bet-the-company risks that belong in the boardroom.

Studies may disagree as to which are the greatest risks, but every study underscores the concern of business executives that risks are rising.

"It's a whole new ballgame on risk—for countries as well as companies."

Transform, Council on Competitiveness

Global Risks 2008: A Global Risk Network Report

World Economic Forum, January 2008

The World Economic Forum (WEF) highlights major categories of transnational risk—with emphasis on systemic financial risk, food security, supply chains and energy. Globalization has increased the likelihood of a "tragedy of the commons"-type outcome by reducing the incentives for any one actor to address problems like pandemics, pollution or global warming. Interdependency has also increased the probability that a disruption in any one region may have significant global repercussions.

The WEF compared the likelihood of 26 core global risks with their predicted severity in terms of economic loss (measured in U.S. dollars).

1. *Globality*, Harold Srikin, James Hemerling and Arindam Bhattacharya. Boston Consulting Group (Boston: 2008)

Core Global Risks and Predicted Severity

Source: World Economic Forum, January 2008

	Risk	Perceived Likelihood (%-WEF Analysis)	Cost (Severity in Billions of US$)
Economics	Food Insecurity	5-10	50-250
	Oil and Gas Price Spike	10-20	250-1,000
	Major Fall in US$	7-12	50-250
	Slowing Chinese Economy (6%)	7-12	250-1,000
	Fiscal Crises in Advanced Economies	1-5	50-250
	Asset Price Collapse	17-22	>1,000
Geopolitics	International Terrorism	5-10	10-50
	Collapse of Nuclear Proliferation Treaty	7-12	5-25
	Interstate and Civil Wars	5-10	50-250
	Failed and Failing States	10-20	30-150
	Transnational Crime and Corruption	5-10	50-250
	Retrenchment from Globalization (Developed)	5-10	>1,000
	Retrenchment from Globalization (Developing)	7-12	50-250
	Middle East Instability	10-20	150-625
Environment	Extreme Climate Change Related Weather	7-12	50-250
	Heat waves and Droughts	7-12	50-250
	Loss of Freshwater	5-10	10-50
	Natural Catastrophe: Cyclone	1-5	50-250
	Natural Catastrophe: Earthquake	1-5	50-250
	Natural Catastrophe: Extreme Inland Flooding	1-5	30-150
Society	Pandemic	5-10	250-1,000
	Infectious Disease, Developing World	3-8	50-250
	Chronic Disease, Developed World	10-20	150-625
	Liability Regimes	5-10	50-250
Technology	CII Breakdown	7-12	150-625
	Emergence of Nanotechnology Risks	1-5	10-150

Risk 2018: Planning for an Unpredictable Decade
Economist Intelligence Unit, 2008

In 2008, the Economist Intelligence Unit (EIU) surveyed 600 senior-level executives to evaluate and rank which risks they believed would present the most significant threats to business during the next decade, as well as the level of preparedness of their individual organizations to address each risk.

High Risk/Impact with Less than High Readiness

- Climate change
- Retrenchment from globalization
- Oil price shock
- Instability in Middle East
- Asset price collapse
- International terrorism
- Emergence of disruptive business mode

High Risk/Impact with High Readiness

- Unexpected regulatory change
- Global recession
- Increased competition from emerging market economies
- Talent shortages

The EIU survey noted that: "Risk management appears to be a function in transition. While it retains its responsibilities as a source of assurance that ensures regulatory compliance and helps the organization to avoid loss, it is now expanding beyond this traditional heartland to assume a broader role. Among our survey respondents, there is general agreement that risk management will encompass more strategic activities over the next ten years, with two-thirds expecting an increase in the use of risk management as a strategic tool."

Risk management and controls now have two parallel dimensions: the traditional "keep me out of trouble" side of risk and the emerging "make my business better" aspect. Managing risk effectively can help improve performance, help improve process and strengthen competitive advantage.

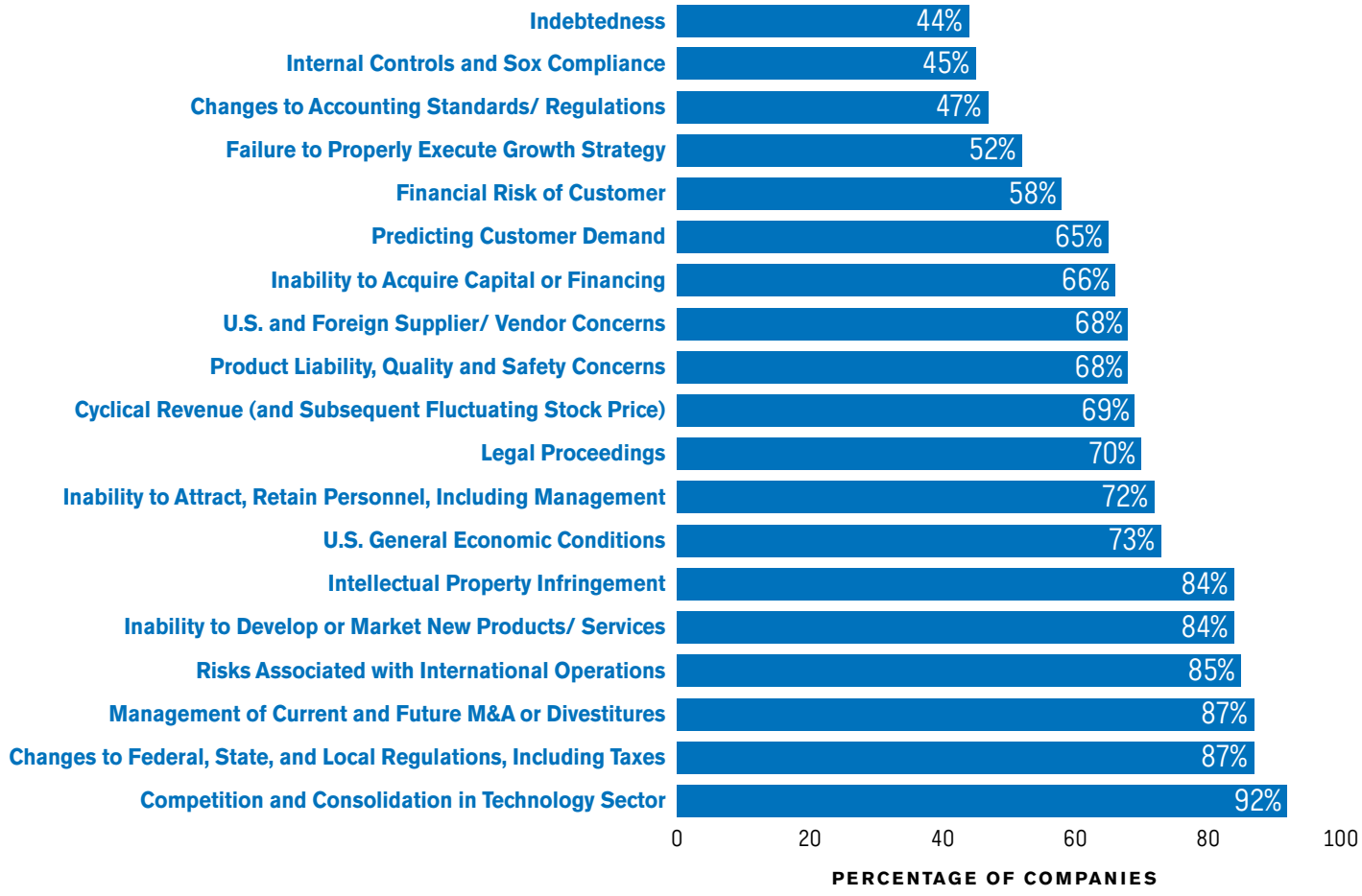
Strategic Business Risks 2008
Ernst &Young

Interviews with more than 70 analysts across 20 disciplines by Ernst & Young captured a different set of insights on key risks.

- Regulatory and compliance risk
- Global financial shocks
- Aging consumers and workforce
- Inability to capitalize on emerging markets
- Industry consolidation/transition
- Energy shocks
- Execution of strategic transactions
- Cost inflation
- Radical greening
- Consumer demand shifts

Top 20 Risks U.S. Tech Companies are Losing Sleep Over

Soure: CMP Techweb, May 28, 2008. Based on an analysis of 10K filings.



Briefing Materials

Capturing Value from Risk Intelligence and Resilience

Overview

A key theme is that risk management is not just about minimizing losses, but about preserving shareholder value and growing the top line. The first wave of studies extended the lens beyond simply calculating immediate losses from failure in risk management. They linked risk management to long-term earnings and shareholder value. A next wave of studies is needed for a more rigorous examination of the upside potential for value creation.

Disarming the Value Killers

Deloitte & Touche, 2005

The Deloitte study found that many of the largest losses in value among the world's largest global companies resulted from their failures to manage risk effectively and systemically. Almost half of the 1,000 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. Roughly one-quarter took more than a year for their share prices to recover, sometimes much longer. By the end of 2003, share prices for one-quarter of these companies had not recovered to their original levels.

"A risk-intelligent enterprise knows when to avoid danger and when to take a chance. It doesn't just stay in business. It prospers."

James Quigley, CEO Deloitte
Fortune Magazine, "Weathering Any Storm", March 19, 2007

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.

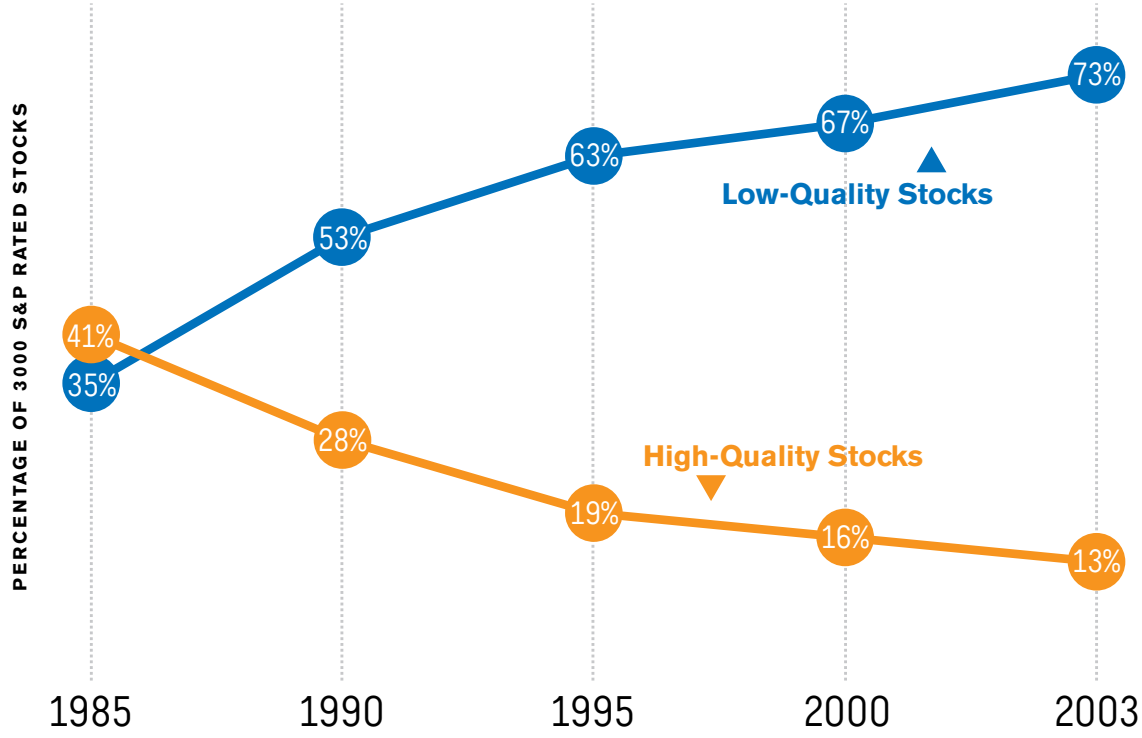
Countering the Biggest Risk of All

Adrian Slywotzky and John Drzik
Harvard Business Review, April 2005

The evidence of strategic risk is becoming ever more apparent. In the past 20 years, there has been a dramatic decrease in the number of stocks receiving a high quality rating by Standard & Poor's and a dramatic increase in the number of low-quality stocks. From 1993-2003, more than one-third of Fortune 1000 companies lost at least 60 percent of their value in a single year.

Many firms have been adopting the practice of enterprise risk management—focusing on financial, hazard and operational risks—but most managers have not systemically addressed the strategic risks

Strategic Risks are Growing
Source: Harvard Business School Review, April 2005



Note: High-quality stocks include those rated A+, A and A-. Low quality stocks include those rated B, B-, C and D.

that can be a more serious cause of value destruction. The authors categorize strategic risk into seven major classes: industry, technology, brand, competitor, customer, project and stagnation.

Managing for strategic risks can often turn defensive moves into offensive opportunities. Besides limiting the downside, strategic risk management helps managers improve the odds of success by forcing them to think more systematically about the future and helping to identify opportunities for growth.

Airbus's focus on a collaborative model that would help its member companies to escape shrinking margins enabled it to create sufficient market share to become a true rival to Boeing. For American Express, the fundamental change in its brand investment mix, in response to competitive threats from other bank cards, set off a decade of growth. For Target, shifting its focus to a customer segment that was different from Wal-Mart's not only helped it sidestep a new competitor but sparked profitable growth.

While managers often see a trade-off between risk and reward, creative risk management combined with a good business model can allow a company to improve in both areas. This is analogous to the evolution, 30 years ago, from a cost-quality trade-off to total quality management which achieved lower costs and higher quality simultaneously.

The Effect of Supply Chain Disruptions on Long-Term Shareholder Value, Profitability and Share Price Volatility

Vinod Singhal and Kevin Hendricks
The Logistics Institute 2005

Researchers looking at the impact of supply chain disruptions found that such events can be catastrophic for businesses and their shareholders. Based on a sample of more than 800 companies that announced a supply chain disruption between 1989 and 2000, 33-40 percent experienced lower stock returns than their industry peers, regardless of industry, cause of disruption or time period. Such firms experienced 7 percent lower sales growth and 11 percent higher costs.

The study shows that firms that experience disruptions, on average, experience a 107 percent decrease in operating income, 114 percent decrease in return on sales, and 92 percent decrease in return on assets. Changes in operating income, sales, total costs and inventories remained negative in the two years after the problems were disclosed.

Innovators in Supply Chain Security: Better Security Drives Business Value

Stanford and Manufacturing Research Institute, National Association of Manufacturers, 2006

International trade is no longer just about moving goods quickly and cheaply. In this age of global terrorism, there is a third element: it is about moving goods quickly, efficiently and securely. Some of the implications of the 9/11 events include an increase of 15 percent in airfreight costs and an increase of 20 percent in the costs of commercial insurance premiums to about $30 billion per year. New security measures following 9/11 are estimated to cost the U.S. economy alone more than $150 billion, of which $65 billion is for changes in supply chains.

The study also quantified benefits, through case studies of eleven major manufacturers and three logistics providers, that have the potential to offset or exceed the costs of security, including:

- Improved product safety (38 percent reduction in theft/loss/pilferage, 37 percent reduction in tampering);
- Improved inventory management (14 percent reduction in excess inventory, 12 percent increase in reported on-time delivery);
- Improved supply chain visibility (50 percent increase in access to supply chain data, 30 percent increase in timeliness of shipping information);
- Improved product handling (43 percent increase in automated handling of goods);
- Process improvements (30 percent reduction in process deviations);
- More efficient customs clearance process (49 percent reduction in cargo delays, 48 percent reduction in cargo inspections/examinations);
- Speed improvements (29 percent reduction in transit time, 28 percent reduction in delivery time window);
- Resilience (close to 30 percent reduction in problem identification time, response time to problems and in problem resolution time); and
- Higher customer satisfaction (26 percent reduction in customer attrition and 20 percent increase in number of new customers).

The New Religion of Risk Management

Peter Bernstein
Harvard Business Review, March-April 1996

The notion that the future rests on more than just a whim of the Gods is a young idea. More than any other development, the quantification of risk defines the boundary between modern times and the rest of history. What have we gained in the transformation from superstition to the supercomputer? We must consider the possibility that breaking free from the Fates has turned us into slaves of a new kind of religion, a creed that is just as implacable, confining and arbitrary as the old.

All but two of the risk management tools we employ today, from the strict rationality of game theory to the challenges of chaos theory, stem from developments between 1654 and 1754. These methods allow people to take more risks than they otherwise would—a benefit to society which cannot progress without risk takers. Without the laws of probability, no great bridges would span our widest rivers, polio would still be crippling children and no airplanes would fly. Without fire insurance, only the wealthiest could afford to own homes. The great capital-intensive industries of our age, such as the railroads and electric power, would have been inefficient creations of the state or not developed at all.

But, there are inherent risks in our risk management tools: the exposure to discontinuity, the arrogance of quantifying the unquantifiable and the threat of increasing risk instead of managing it.

Discontinuity The amazing stability of key relationships depletes the capacity of people to imagine anything different. Many calamities are not unpredictable; they have just become unthinkable.

Quantifying the Unquantifiable How can we instruct a computer to model events that have never occurred? Instead, we only program past data, limiting our deliberations to the variables that lend themselves to quantification.

Increasing the Risk Our faith in risk management tools encourages us to take risks, but we should be wary of increasing the total amount of risk. Seat belts can cause drivers to behave more aggressively. Derivative instruments to hedge risk have become vehicles for high-speed sleigh rides. Diversification is no guarantee against loss, only against losing everything at once.

Nothing is more soothing and authoritative than the screen of the computer with its imposing arrays of numbers, luminous color schemes and artfully composed charts. We tend to forget that we are operating a gadget whose mind is at rest. Computers exist to answer questions, not to ask them. Whenever we allow ourselves to ignore that truth, the computer becomes the ally, rather than the enemy, of our conceptual errors.

The Business Value of Resilience

Council on Competitiveness, *Transform.*
Company Vignettes

Wal-Mart

Wal-Mart's reputation for supply chain gymnastics was showcased during Hurricane Katrina, when the company 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. But, its supply chain sophistication was not developed as a disaster management tool—and in fact, the investment could not have been justified solely on disaster preparedness grounds.

The inventory visibility and supply chain agility is rooted in a business model that requires quick changes in the merchandise mix as a source of competitive advantage and new business opportunities, and robustness in its information and logistics systems. Resilience has been embedded in the company's DNA to handle peak requirements.

Georgetown

The availability of student housing is a critical part of the university's business continuity. If housing is not available, then one of the main sources of operating revenue—tuition—is also at risk. 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 took these savings and increased its business interruption insurance fivefold (well before Katrina). That became a positive factor in determining the university's rating and cost of capital in a subsequent bond issue.

Waste Management

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 security, including reduced fraud and new tools for work process efficiency and safety. New business opportunities have included a "witnessed and certified" product destruction service, and security contracting for small and medium size companies. The security center has gone from an overhead expense to a profit center for the company.

Briefing Materials

Implementing Risk Intelligence

"Risk comes from not knowing what you're doing."
Warren Buffett

"A little risk management saves a lot of fan cleaning."
Unknown

Overview

How firms should manage risk remains a hotly debated topic. Enterprise Risk Management (ERM) was assumed to be the best practice…at least until the subprime crisis. What seems clear is that, even despite the debacle, the tools, talent and processes for market and credit risk management are still more sophisticated than those available for operational risk or strategic risk management.

The literature on ERM seems to fall into three separate categories:

1. ERM is a good approach, but it has never been fully implemented and risks remain siloed;
2. ERM is fundamentally flawed; the approach ignores risk intelligence in favor of risk assessment. Business managers on the ground are in a far better position to sense and understand risk than a headquarters-based risk management system; and
3. ERM approaches, even if well implemented, are incomplete. Perfect risk management will still be ineffective if the processes are not linked to governance, strategic planning and value creation.

ERM Just Needs to Be Fully Implemented

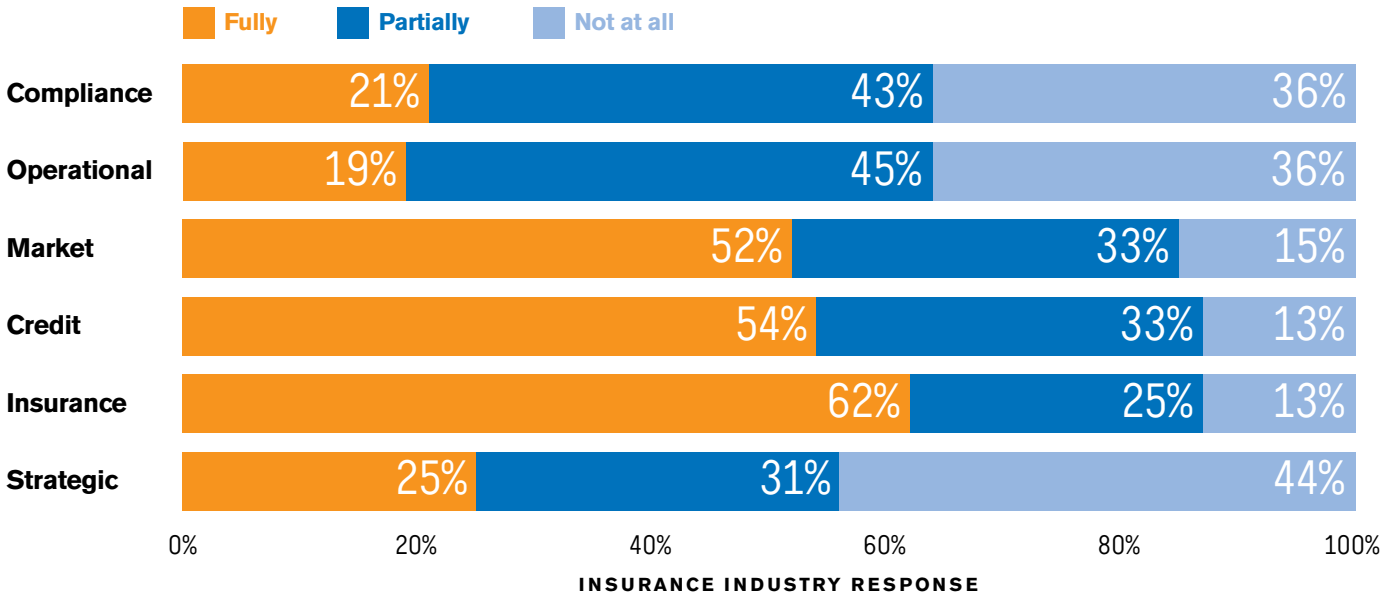
Does ERM Matter? Enterprise Risk Management in the Insurance Industry
PriceWaterhouse Coopers, June 2008

Key findings from a survey of 53 insurers:
The extent to which ERM is integrated into the day-to-day decision-making and frontline risk-taking of businesses is often limited. Less than half of the survey participants are confident that ERM has been embedded into their strategic planning, resource allocation and performance management.

"Ultimately, this lack of integration means that ERM programs may simply be perceived as an additional layer of bureaucracy within the business rather than being integral to how it is run."

The poor quality of risk data and limited usability of model analysis do not provide a strong basis for decision-making. Less than 40 percent of respondents believe that their risk data and systems are good or excellent. Nearly half believe that their risk information does not support their risk objectives. The survey group saw ERM systems as even less efficient in anticipating emerging risks.

Level of ERM Development and Implementation
Survey responses from Insurance Industry
Source: PriceWaterhouse Coopers



What Is Enterprise Risk Management?

Risk management has increasingly come to be identified with enterprise risk management processes. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) described eight components of ERM systems:

Internal Environment The internal environment sets the basis for how risk is viewed, including the risk management philosophy, risk appetite, integrity and ethical values, and the environment in which they operate;

Objective Setting Objectives must exist before management can identify potential events that could disrupt their achievement;

Event Identification Internal and external events affecting achievement of the objectives must be identified, distinguishing between risks and opportunities;

Risk Assessment Risks are analyzed, considering likelihood and impact;

Risk Response Management selects risk responses—avoiding, accepting, reducing or sharing risks—and a set of actions to align risks with risk tolerances;

Control Activities Policies and procedures are established and implemented to help ensure risk responses are effectively carried out;

Information and Communication Relevant information is identified, captured and communicated in a form and time frame that enable people to carry out their responsibilities; and

Monitoring The entirety of enterprise risk management is monitored and modifications are made as necessary.

Five Barriers to an Enterprise View of Risk

Gartner, July 27, 2006

In a survey of 61 business and IT executives operating the retail, energy, financial services, health care and public sector industries, the Gartner Group identified five major roadblocks to ERM:

- Growth trumps risk management as a budgetary priority;
- Risk is subjective—views are siloed and personalized;
- There are multiple, conflicting risk agendas;
- Stakeholders struggle with risk relevance—related both to the success of individual efforts and broader organizational goals; and
- Lack of information is the primary barrier to a transition from silo-based to systems-based risk management.

Top 10 Enterprise Risk Management Myths
Gordon Burnes, Vice President, Open Pages
Financial Executive, May 2008

10. IT Risk Management = Information Security
    Most information management programs place too much emphasis on the how and what, and far too little on the why. Information risk management is all about why.
9. CIOs Are Strategically Driving Enterprise GRC Solutions
    In purchasing compliance platforms, IT is too often at the table in a support role rather than as an advisor on the long-term strategic benefits of a common GRC platform for managing both risk and compliance.
8. One Size Fits All Approaches Work
    ERM has to be tailored to an organization's corporate strategies, business activities and external environment; standardized methodologies will likely fail.
7. Risk Can Only Be Managed from the Center
    Responsibility for risk management has to be pushed through the organization; accurate information lies at the business line level.
6. Risk and Compliance Can Be Managed by Spreadsheets
    Spreadsheets are manually intensive and highly reliant on the individuals who manage the process. Linking, updating and archiving data in spreadsheets is mostly ad hoc.
5. Traditional Audit Planning Accurately Assesses Risk Factors and Frequency
    Progressive organizations are turning toward a more agile, top-down approach to risk assessment to drive audit scheduling and frequency.
4. Enterprise Risk Management Is Dead
    Today's control-based ERM frameworks have a bias for analysis over action, and the production of documentation sometimes trumps managing risk. ERM should be deployed bottom up, so that business managers are the first-line risk mangers.
3. Risk Management Just Takes Common Sense
    As business activities have become more complex, so has risk management, which now covers a wide variety of disciplines. It may not be rocket science, but it requires sophisticated models and analytics.
2. TJX–It Can't Happen Here
    Preventative technology and knowledge get better every day, but so do the villains. Every organization is susceptible to a breach.
1. You Cannot Plan for the Unknown
    Key risk exposures do not always follow a normal distribution. You may not be able to predict them, but you can plan for the events that lie outside the realm of expectations.

The ERM Approach Is Fundamentally Flawed

The Board's Neglected Risk Responsibility

David Apgar
Directorship, February 2008

Efforts to market ERM as a brave new discipline have made confusing what was once clear. The manager directly responsible for an operation—be it sales, production, procurement, design or planning—is the best source of information about its risks. ERM can tell you which manager-identified risks the firm can hedge, but it can never discover new ones, such as geopolitical risks that no manager has identified.

Apgar's theory of risk (from his book, *Risk Intelligence: Learning to Manage What We Don't Know*, Harvard Business School Press, 2006) focuses on "learnable" and "random" risks. He maintains that most of the current tool set deals with random risks for which no competitor has an inside track or relative advantage. It is the non-random, learnable risks—involving behaviors, technologies, marketing strategies and supplier relationships—that can put companies at a comparative disadvantage.

For Apgar, the key concept is not just strengthening the capabilities for centralized risk management, but improving the Risk IQ of managers.

- Many (if not all) non-financial risks are learnable: forecasts of customer demand for new products, services and attributes; security and political conditions; the actions of competitors, regulators and suppliers; capacity and loyalty of workers; creditworthiness of counter-parties; and the effectiveness of new technology.
- While uncertainty underpins all types of risk, managers can differentiate between random risks and learnable risks. Risk assessment tools should evaluate the quality of a business manager's risk information resources, not just the magnitude of the risk. Apgar argues that knowledge about the operating team is the best predictor of how it will handle challenges.

This approach to risk has some key implications for CEOs and boards.

- CEOs and boards should be focused on risk intelligence rather than risk assessment. A company can get into more trouble by selecting risks it is not well-equipped to manage than it can by merely taking on risks that appear large.
- Learnable risks raise competitiveness issues. Random risks do not. This means that an organization might overprotect itself relative to a competitor—or fail to move up the learning curve as fast as its competitor—and create a cost disadvantage for itself. The assumption that worst-case loss depends on only exposure is wrong. It also depends on what is known and who else is taking the risk.
- Boards and CEOs should focus on tools to evaluate the ability of line managers to assess risk.

The ERM Concepts Are Incomplete—Missing Some Key Components

Time to Bail on ERM?

Treasury and Risk, June 2008

What is missing in ERM systems are the linkages to corporate strategy. Risk management still has to go from the back room to the board. Specific risks are not always related to strategic risks. (Subprime issues were not even on the radar screen in housing-related industries). Chief risk officers need more than a dotted line reporting to the board or audit committee. There needs to be a clear link between corporate strategy, risk appetite and financial and operational plans. Risk professionals need to have the independence and stature to be able to voice concerns—to close the gap between risk management and business management.

Integrating Governance, Risk and Reporting to Create Long-Term Value

Brian Ballou and Dan L. Heitger, Strategic Finance, May 1, 2008.

What is missing is an integration of three traditionally disparate topics—corporate governance, enterprise risk management and business reporting. Some organizations structure risk management so that executives who own the process, often titled chief risk officers, report directly to the board. Other organizations structure risk management so that executives who own the process report to the board's risk committee—or even an executive risk committee—on a nonsystematic basis. A key determination in how organizations implement governance mechanisms to manage risk is the extent to which they have linked risk management to the organization's mission and strategies. Overall, organizations differ greatly in their emphasis. Some emphasize governance if they have prestigious board members who are in high demand. Others emphasize more sophisticated processes for risk management, particularly in regulated industries where they are evaluated on that basis. Organizations that face high levels of media scrutiny typically have more sophisticated processes for monitoring and reporting how effective they are at managing particular risks (death or injury of workers). But very few organizations link their risk management processes to their strategic decision-making processes.

Issues in integrating corporate governance, risk management and business reporting:

- Assure board oversight of structures to manage risks and report on risk management effectiveness;
- Develop a common risk language across organizational silos;
- Link risk to strategy, creating a portfolio that helps management seek opportunities and mitigate risks where appropriate;
- Implement steps of risk assessment—understanding sources, probabilities, impacts and prioritizing risks within a common framework;
- Respond to risk and understand how choices impact other risks;

- Measure risk responses, residual risk and impact on performance;
- Report risk management information to internal stakeholders;
- Understand external demand for risk management information; and
- Report risk management information to external stakeholders.

Marrying Risk and Strategy to Create Value

Peter Pourquery
Boston Consulting Group, 2007

In a survey of risk management practices, BCG found that managing risk and formulating strategy remain segregated at a majority of banking institutions. Collaboration between the functions is hampered by organizational structures that calcified years ago, when risk experts were confined to more traditional roles.

Pourquery used a historical example to illustrate his point. In January 1777, General George Washington and Lord Cornwallis gathered their advisors on the eve of battle. Cornwallis presided over a small hierarchical gathering that was described as "less council than court". Washington's council was more open and mixed: "Local citizens were invited to attend and speak freely; Washington did not propose a single course of action but framed a problem. Even before a single shot was fired, the outcome was largely decided by how well—or poorly—these leaders tapped their experts, assessed their risks and used that understanding to inform strategy."

Key findings

- Managers of business lines want their bank's risk managers to integrate closely with business teams and to act less like internal police and more like strategic advisors;
- More than half of survey respondents would like their risk functions to provide a range of services beyond the traditional purview, contributing to areas such as business strategy and planning and marketing and business development; and
- CRO's reported that banks continued to exclude risk managers when they convened their own councils of war.

Recommendation

Include risk experts in the development of long-term strategy, for example, by appointing the chief financial officer, the chief risk officer and the head of strategy to a committee charged with exploring strategy within the context of management risk and economic capital.

Other Issues that ERM Systems Are Missing Altogether or Not Effectively Addressing

Reputation and its Risks

Robert Eccles, Scott Newquist, Roland Schatz
Harvard Business Review, February 2007

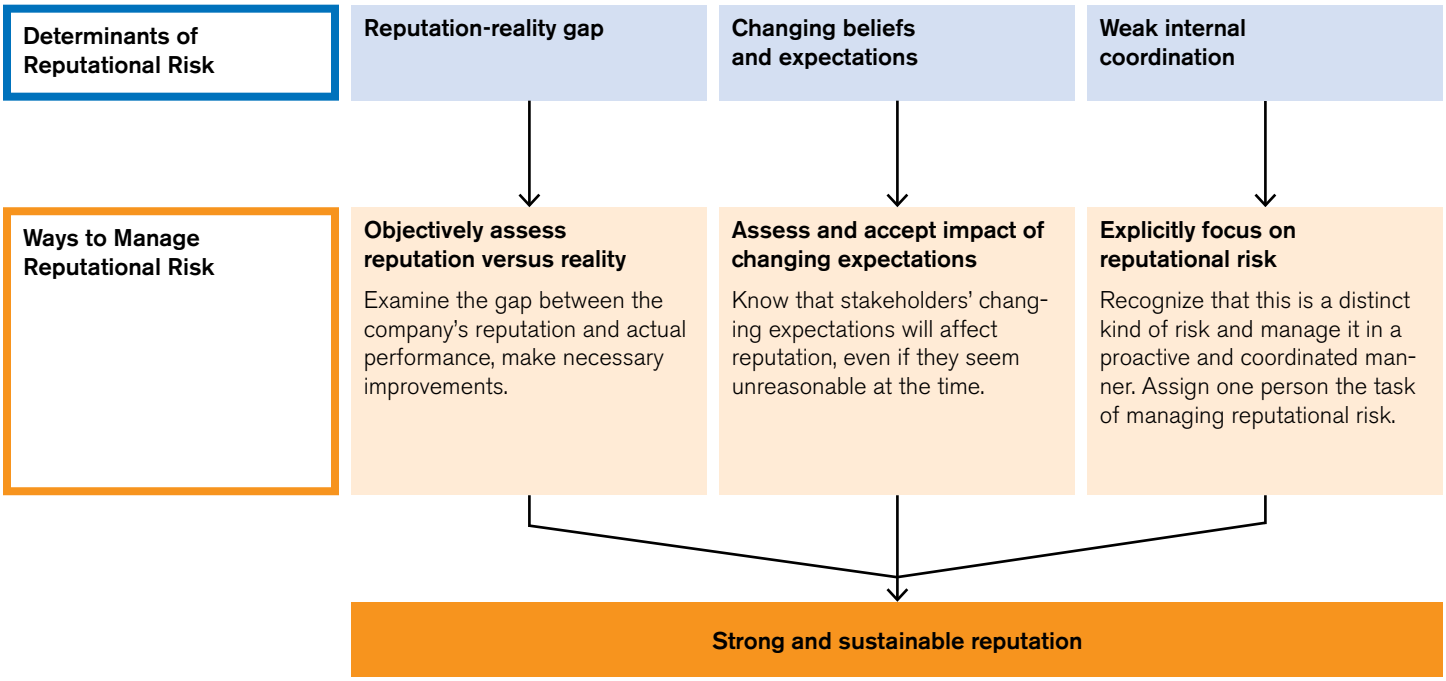
Most companies do an inadequate job of managing the risks to their reputation. The tendency to focus on the threats that have already surfaced is not risk management, but crisis management. When 269 executives were surveyed by the

Economist Intelligence Unit in 2005, 84 percent responded that their CEOs were principally responsible for managing reputational risk—effectively saying that no one manages reputational risk on a day-to-day basis. The authors pointed to three determinants of reputational risk:

- A gap between reputation and reality (e.g. Texas city refinery and Prudhoe Bay problems were at odds with the Beyond Petroleum and due diligence messages);
- Changing beliefs and expectations (GSK suing the South African government for patent infringement on retrovirals); and
- Weak internal coordination among different business units or functions (AMR union wage reductions simultaneous with bonuses for senior managers).

A Framework for Managing Reputational Risk

Understanding the factors that determine reputational risk enables a company to take actions to address them.
Source: Harvard Business Review



Navigating in the Midst of More Uncertainty and Risk

Jim Butcher, Nick Turner, Gerard Drenth
Journal of Applied Corporate Finance, Fall 2006

What is missing is the scenario-building capacity that enables out-of-the-box thinking to anticipate strategic risks. Even as companies are deploying enterprise risk management systems, risks continue to multiply and move into more strategic and macro-event risk arenas. The consequence has been an expansion of traditional risk management tools into realms of greater uncertainty, where managers quickly run up against the limits of quantitative methods and models.

University of Chicago economist Frank Knight distinguishes between risk and uncertainty. Risk applies to cases where the distribution of possible outcomes is either known or can be estimated. Uncertainty is about a potentially unlimited set of choices and a unique situation. Many risks are actually turning out to be "uncertainties" and require new approaches.

The authors describe the use of scenario planning as a valuable tool to navigate between risk and uncertainty, citing four key benefits:

- Breadth and Diversity of Experience
  The tyranny of conventional wisdom and uncritically accepted mental models can blind executives to important changes in an industry and macro-environment. One of the real values is to consider the broader context and how it is changing before drawing key business insights;
- Pattern Recognition
  Scenario work has the potential to "envision" new patterns that may emerge, rather than simply relying on past patterns;
- Right Answer, but Wrong Timing
  A late 1990s scenario about a major financial institution that could not settle was not needed for Y2K, but it created institutional memory and preparedness for a post 9/11 response; and
- Mental Models and Leadership
  One of the real accomplishments of scenario planning has been to create more flexibility in executives' thinking—and a willingness to be more forward-thinking.

Stemming the Rising Tide of Supply Chain Risks

Marsh, April 2008

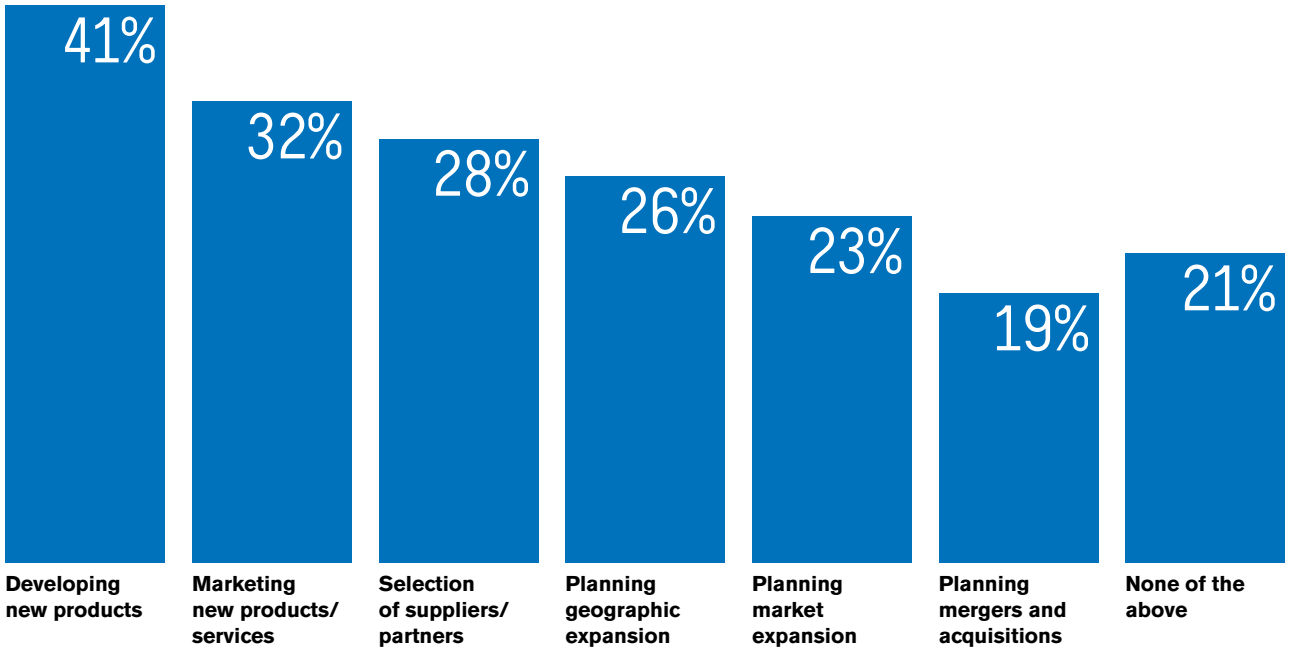
Nearly three-quarters of the 110 risk managers surveyed say their companies' supply chain risk levels have increased since 2005—and 71 percent report that the financial impact of supply chain disruptions has also increased—damaging bottom lines, customer retention and brand equity. None of the risk managers surveyed said that their company is highly effective at supply chain risk management today, and just 35 percent said they were moderately effective. Today, the typical risk manager estimates that just 25 percent of his or her company's end-to-end supply chain is being assessed annually for risk likelihood and impact.

Under the Spotlight: The Transition of Environmental Risk Management
Economist Intelligence Unit, 2008

What is missing is environmental risk management. One-third of companies manage environmental risk in an ad hoc fashion. Another 26 percent manage it in a coordinated way, but without ties to overall risk management. And 10 percent have no management structure for environmental risk.

Survey respondents report that there is no clear consensus about who is responsible for environmental risk. Many companies conduct strategic activities without a formal assessment of environmental risk.

Formal Consideration of Environmental Risk
Source: Economist Intelligence Unit



Briefing Materials

Reaching for Resilience

Overview

Enterprise resilience represents a new thrust in the effort to anticipate and adapt to turbulence and to assure effective risk management, disaster recovery, business continuity and profitability.

The scientific meaning of resilience refers to the properties of a material to resume an original shape after being bent or stretched. Different authors and organizations have expanded this original focus and definition to preparedness for disruptions large and small: critical infrastructure protection; part of homeland and economic security; sustainability; enterprise risk management; and corporate competitive advantage.

The problem is that the word resilience has so many meanings that it risks becoming meaningless. The Department of Homeland Security uses the term to mean preparedness to recover from catastrophic disruptions, but in practice, homeland resilience tends to look strikingly like homeland security. A number of vendors use the term resilience interchangeably with IT security, supply chain security, disaster recovery or business continuity.

"It's not the strongest of the species that survives; not the most intelligent… It's the one that is the most adaptable to change."

Charles Darwin

In Australia, the resilience framework is societal, recognizing interdependence among individuals, organizations and communities. Even the most resilient organization will not be able to meet its goals if the local infrastructure is unable to resume functioning or individuals are not resilient enough to return to normalcy and jobs.

The goal is not just recovery or continuity, but the transformation from reactive to proactive to adaptive—and a set of principles and best practices that enable the transformation.

Properties of Resilience: The Four Rs

MCEER, University of Buffalo

Robustness Strength, or the ability of elements, systems and other units of analysis to withstand a given level of stress or demand without suffering degradation or loss of function.

Redundancy The extent to which elements, systems or other units of analysis exist that are substitutable, i.e., capable of satisfying functional requirements in the event of disruption, degradation or loss of function.

Resourcefulness The capacity to identify problems, establish priorities and mobilize resources when conditions exist that threaten to disrupt some element, system or other unit of analysis. (Resourcefulness can be further conceptualized as consisting of the ability to supply material—i.e., monetary, physical, technological and informational—and human resources to meet established priorities and achieve goals.)

Rapidity The capacity to meet priorities and achieve goals in a timely manner in order to contain losses and avoid future disruption.

Enterprise Resilience: Managing Risk in the Networked Economy

Starr, Newfrock and Delurey
Strategy+Business, 2003

During the last half century, the vertically integrated company has given way to the networked enterprise. Successful firms today must deal with intertwined layers of information, raw materials, analytical data, customer communication and service and network infrastructure—at unprecedented speed—while maintaining countless secure relationships with suppliers, technology outsourcers and government regulators.

Enterprise Resilience (ER) versus Enterprise Risk Management (ERM)

Risk management models have not kept pace with the shift from centralized to networked organizations. Most ERM programs rely on "point solutions," attempting to moderate risks by "hardening" potentially vulnerable spots. Conventional ERM fails to account for interdependencies across vertical and horizontal operations that characterize the networked world. In contrast, enterprise resilience planning creates an integrated first line of defense and an offensive strategy to guard the entire extended enterprise against new, unavoidable risks that are the byproducts of interdependent operations. Resilience focuses on creating organizations that are "sensing, agile, networked and prepared", focused on "how to survive before the fact".

Redefining the Corporate Governance Agenda: From Risk Management to Enterprise Resilience

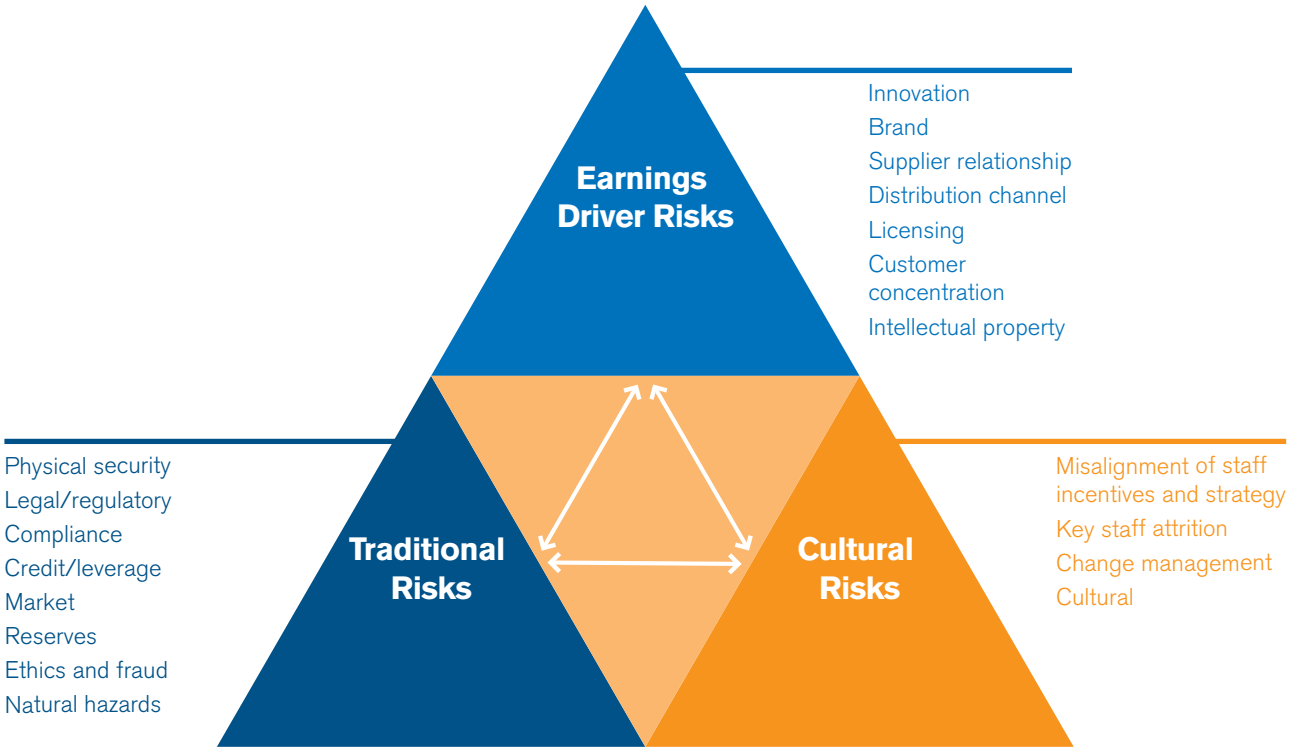
Booz Allen Hamilton & Weil, Gotshal & Manges, 2004

What is missing is the bridge from risk intelligence to enterprise resilience. Traditional risk management systems and solutions are inadequate to handle today's expanded spectrum of market and business risk. As the rate of change in the market accelerates, companies require an adaptive risk management approach that both responds to and anticipates business shifts. Very few companies have managed to develop a dynamic capability for enterprise resilience.

Enterprise resilience is predicated on an expanded view of risk—one that focuses on value and therefore encompasses not only traditional risks (e.g. financial, natural hazard, physical security, legal compliance) but also risks related to earnings drivers (e.g. innovation, intellectual property, partnerships) and company culture. Enterprise resilience marries risk assessment, information reporting and governance processes with strategic and business planning to create an enterprise-wide early warning capability that is embedded in the day-to-day business operations and culture of the firm.

Enterprise Resilience Expands the View of Risk

Source: Booz Allen Hamilton



Four Steps to Corporate Resilience
Liisa Valikangas
Strategy+Business, 2004

The author argues against the conventional wisdom that corporate failure and death are essential to economic health, and questions the logic that start-ups can replace the wisdom and wealth accumulated by a more mature company. Rather than survival of the fittest, a truly healthy approach to economic adaptation and wealth creation is for companies to become more resilient.

Four ways that companies can build the capacity to continually renew themselves include:

Rethink Underlying Principles of Management Decision-Making
Managing a resilient corporation requires a greater willingness to access information from multiple sources and to avoid guidance by those with a vested interest in the status quo;

Generate a Portfolio of Strategic Options
Resilient companies build a portfolio of experimental strategies from all parts of the company. Some portion of capital expenditures—30 percent or so—should be earmarked to test new strategies and innovate aspects of the company business model;

Careful Examination of Resource Allocation
Most companies create budgets based on a legacy principle: if you have been successful, you deserve funds in the future. A more resilient solution is to manage resources so that funding for known opportunities is balanced by an appetite for new ventures; and

Implement More Effective Corporate Governance
Directors have to make sure that management has a plan for the future that does not just relive the past but provides the right resources to promote resilience.

Living on the Frontline: The Resilient Organization
KPMG Business Continuity Centre of Excellence, 2007

In the evolution toward "the resilient organization", there are three mutually dependent challenges: People, Diversity and Coordination.

People Come First. Five focus areas include:
1. Accounting for people immediately after a disaster;
2. Effective communication with staff and family members through the recovery process;
3. Developing a clear understanding of where corporate and individual responsibilities lie in various scenarios;
4. Developing a better understanding of the human impact of major disasters; and
5. Increasing flexibility through cross-training in order to resource "spikes" in demand.

Diversity of Solution. Three key aspects highlighted:
1. Greater use of remote working capabilities;
2. Setting up split-site operations for larger-scale critical functions; and
3. Enabling the transfer of critical operations to other global locations without depending on significant staffing from the affected location (moving the work, not the people).

Coordination with the Public and Private Sectors. Key issues include:
1. Sharing experience with other firms;
2. Anticipating planning for supply chain disruptions;
3. Regular communication with regulators, civil authorities and emergency services; and
4. Participation in market-wide exercises and benchmarking activities.

The Resilient Enterprise

Yossi Sheffi
MIT Press, 2005

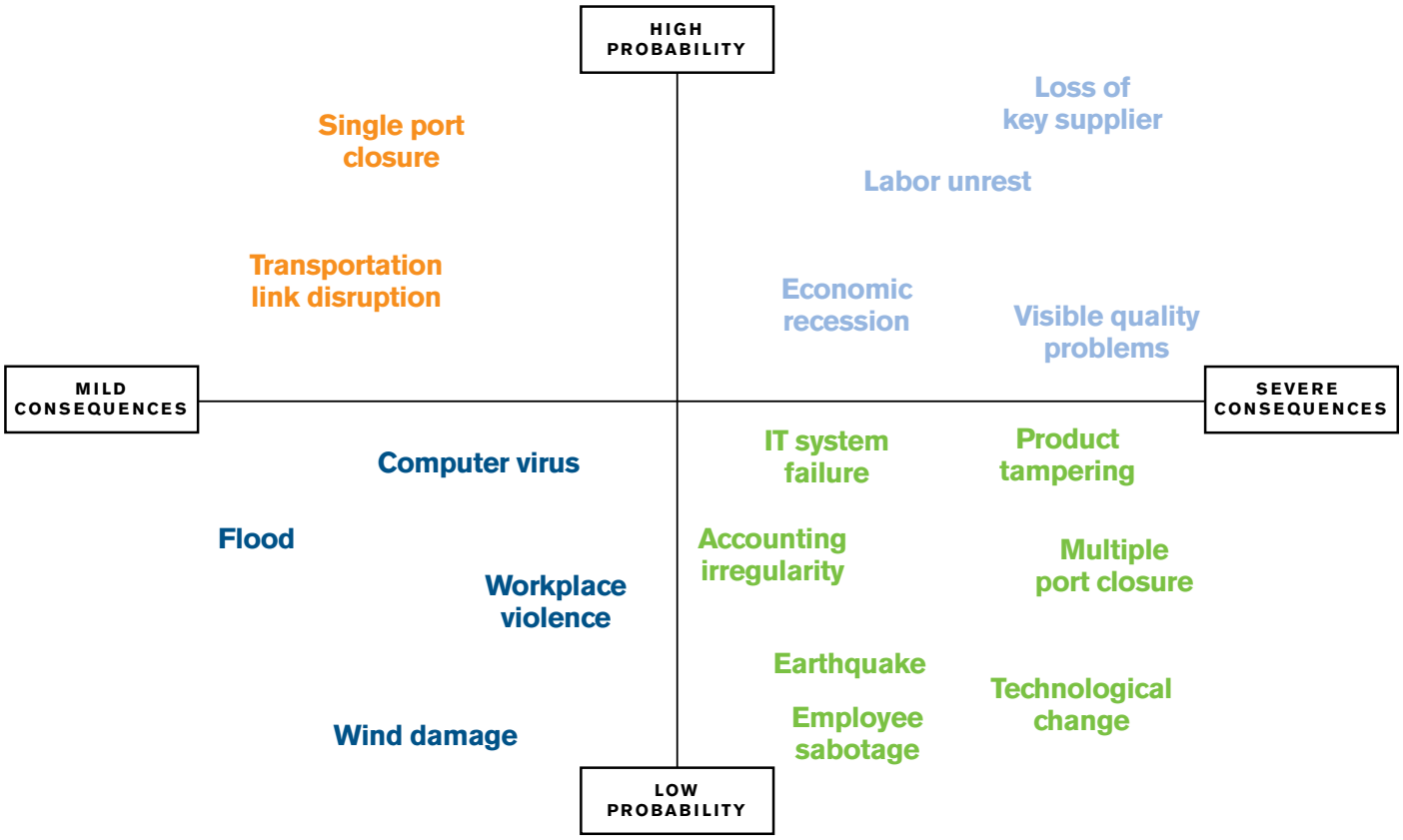
Companies are now exposed to a multitude of unexpected events—from natural disasters such as earthquakes to terrorist attacks and supplier failures. They not only need to become more resilient to these shocks, but they can actually increase their everyday competitiveness and gain strength from such disruptions.

A company can become more resilient by designing its supply chain for robustness. One of the standard ways is to use redundancy, which is expensive. Other ways to make the system more resilient include: forging strong relationships with critical suppliers while developing alternatives for commodity suppliers; working with interchangeable parts; cross-training employees; deploying flexible manufacturing; utilizing concurrent processes of design, manufacturing and distribution; delaying product differentiation downstream in the supply chain so products remain in a fungible state as long as possible; and collaborating with trading partners.

These principles create supply chains that are not only resilient but also flexible and that can respond to day-to-day demand changes. One begets the other, because a supply shortage and a demand spike are, at their core, a problem of supply/demand mismatch. Companies that have built their supply chains to respond to significant demand fluctuations have also built in the ability to respond to supply shortages.

Enterprise Vulnerability Map

Source: The Resilient Enterprise, Yossi Sheffi, MIT Press, 2005



Relationships, Layoffs and Organizational Resilience

Gitell, Cameron and Lim
University of Michigan, September 2005

Resilience in everyday parlance refers to the capability to 'absorb strain and maintain coherence' (Oxford English Dictionary). In organizational science, it refers to A) the maintenance of positive adjustment under challenging conditions, B) the ability to bounce back from untoward events, and C) the capacity to maintain desirable functions and outcomes in the midst of strain. Resilience is a dynamic capacity of organizational adaptability that grows and develops over time. It is not a static attribute that organizations do or do not possess. Rather, it results from processes that help organizations retain resources in a form sufficiently flexible, storable, convertible and malleable to avert maladaptive tendencies and cope positively with the unexpected.

The authors argue that organizational resilience is akin to individual resilience in one key way: resilience grows out of the cohesiveness with a group. They argue that the two key characteristics of resilience are a strong commitment to employees (relational reserves) and the financial resources to maintain those commitments in the face of unanticipated events.

In a study of 10 major airlines after 9/11, the authors demonstrated a negative correlation between the extent of employee layoffs and the recovery of share value during a subsequent three year period. Firms that had announced the largest layoffs recovered less of their stock value, which the authors attributed to the loss of relational reserves between companies and their employees.

They also noted that, although a lack of financial reserves makes an organization vulnerable to crisis and more dependent on layoffs as a coping strategy (and therefore less resilient), Wall Street tends to discourage high levels of financial reserves as a poor use of capital. The example cited was Southwest Airlines, which:

- Laid off no employees and had the fastest stock price recovery;
- Was able to weather the storm because of its strong financial reserves; but
- Southwest's conservative approach had been criticized by Wall Street analysts who argued that the airline should use its extra cash to make acquisitions or buy back stock.

Organizational Resilience

Robert Oldfield, 2007

In an attempt to manage a turbulent environment, most organizations have mature risk, business continuity, security and emergency management programs. Unfortunately, these programs frequently manage turbulence in isolation from each other. Risk managers maintain risk registers. Security managers conduct threat and vulnerability assessments and business continuity managers carry business impact analyses. A resilient organization recognizes the synergies between these functions. It recognizes that a risk is a risk regardless of whether or not it has been identified and regardless of who identifies it.

Resilience is not a plan or a checklist. The elements of a resilient organization are:

- Adaptive Capacity
  Recovery to an original state may not be the best option, and organizations need to be able to adapt to maintain competitive advantage;
- Communications
  Lack of communications has been a contributor to global disasters when those who had the information did not pass it on, or when those in authority did not act on it;

- Interdependencies
  Independent thinking is not suited to interdependent reality. Independent people who do not have the maturity to think and act interdependently may be good producers, but they will not be good leaders or team players;
- Situational Awareness
  Awareness includes understanding risks and vulnerabilities, enabling quick detection of change and rapid response;
- Leadership
  The key elements include principle-centered leadership, non-hierarchical communications and empowerment to act;
- Culture and Values
  Culture is about how principles are learned and translated in day-to-day behavior. Values contribute to the culture and may include integrity, customer focus and results;
- Enterprise-Wide
  All business units and functions contribute to organizational resilience; and
- Ownership
  Resilience is not a word to describe only one of the tactical elements of security, risk or business continuity. It is the balanced integration of all of these.

Business Resilience

The ability to rapidly adapt and respond to risk and opportunities in order to maintain continuity of business operations, remain a trusted partner and enable growth.

Business Resilience for the Global Marketplace: Transforming Operating Risk Into Competitive Advantage
IJet, June 2008

In pursuit of global competitiveness, organizations no longer operate within one country or region. Instead they rely upon a network of partners to build, review, transport or otherwise deliver a better, less expensive, faster-to-market product or service than they could on their own. The lure of the global marketplace is a double-edged sword; there are costs to adequately managing new risks and disruptions.

The tools and processes of risk management have evolved from reactive to proactive to adaptive.

Disaster Recovery
Incident management and disaster recovery initiatives tend to answer the "what if" question. They focus on quick response to disruption: insurance (to transfer risk and pay for recovery); incident reporting (to learn about disruption quickly); and response

plans and response services (to provide aid to people and operations in need). Disaster recovery tends to be reactive in nature.

Business Continuity
Business continuity experts answer the question: "When" our business is disrupted, how will we continue to provide service to our customers? Organizations utilize real-time intelligence, business continuity plans and decision support technology and services to guide fast decisions about what to do next. Business continuity tends to be proactive in nature.

Business Resiliency
Resilience asks how to gain competitive advantage from managing risk. Resilient organizations use predictive intelligence for early warning and situational analysis and historic intelligence to identify and seize new opportunities. They leverage a common operating platform across departments and business units for a global perspective. They routinely communicate with employees, partners and customers. Resilient organizations are adaptive.

Business Resiliency: Moving the Mountain an Inch at a Time
Mary Herbst, May 2008

Mary Herbst, director of business resiliency, described the "Road to Resilience" for Carlson Hotels. Back in 2004, there was no clearly defined plan for business continuity. Accountability was an IT function, not a business function. Plans were written for audit purposes, not for implementation. And, technology planning was scattered and non-specific.

Business Resiliency Model
Source: Mary Herbst

Attributes of a Business Resiliency Program

- Comprehensive
- Well-coordinated
- Integrated
- Measured
- Well-supported
- Funded

During the next two years, risk management processes began to be formalized. Accountability moved from IT to audit business risk management. Technology plans were completed, risk assessments performed, specific governance resources assigned to each operating group, and disaster recovery planning coordinated with business continuity.

Hurricanes Katrina and Wilma dispelled complacency about readiness plans, while the threat of a pandemic triggered a renewed commitment to transform business continuity into business resilience.

- The Resiliency Goal
  Protection of people, assets and brands through planning, risk analysis, risk mitigation, crisis response and the continuity of business and technology.
- Critical Ingredients for Success
  Executive support, operating group ownership, funding, business resiliency councils, strong partnerships, change management processes and the integration of business resiliency into all aspects of the business.

Lessons

- Integrating Business Resiliency in all areas of the business ensures that resources are ready to respond to all critical events;
- Without executive sponsorship, all efforts will dissipate;
- It is a long and winding road;
- There are no "silver bullets";
- It takes commitment from the top and resources from all levels of the organization; and
- When you feel like giving up—remember "why" it is so critical.

National Organizational Resilience Framework Workshop

Australia, December 2007

Australia has begun considering how critical infrastructure protection can evolve into a next generation approach, like resilience.

The words "critical infrastructure protection" create misconceptions in four ways. Critical infrastructure protection is perceived to be:

- Focused on asset protection rather than service delivery;
- Associated with security rather than the continuity of systems;
- Limited to protection of assets rather than a partnership with the emergency management community; and
- Focused on terrorism rather than all disruptions.

Resilience is neither a plan nor a checklist. The capacity is found in an organization's culture, attitudes and values. A resilient organization:

- Is adaptive and can work with or in spite of uncertainty;
- Puts change and adaptation in its vision;
- Foresees the future and acts on it;

Question CEOs Should Ask

What are our key vulnerabilities?

What are our critical interdependencies?

How do we monitor for new threats and incorporate them into our risk practices?

What strategic changes are occurring in our threat environment?

Who would be our leadership team in times of crisis?

How do we ensure all business units work in a united way during a crisis?

How should we ensure all of our staff are informed of our immediate priorities in a crisis?

Do we have a program ready to build and maintain staff morale during response and recovery to a crisis?

Are mutual aid agreements in place with our sector peers?

Which key stakeholders would support us in times of adversity? Which would attempt to undermine us?

- Ensures staff know what to do;
- Understands its interdependencies;
- Makes and seizes opportunity in times of crisis;
- Values the resilience of the community within which it operates;
- Thinks outside the box; and
- Capitalizes on adversity and change.

America the Resilient
Stephen Flynn
Foreign Affairs, March-April 2008

The United States is becoming a brittle nation. When the power goes out, Americans are incapacitated. Two decades of taxpayer rebellion have stripped down emergency preparedness capabilities. Most public health and emergency management departments are not funded adequately to handle routine work. Aging infrastructure compounds the risk of destruction and disruption. One of the rationales for building the interstate highway system was to support the evacuation of major cities if the Cold War turned hot. In 2006, the year the system turned 50, Americans spent a total of 3.5 billion hours stuck in traffic.

What Washington should do, instead of sounding the alarm about apocalyptic terrorist groups, is arm Americans with greater confidence in their ability to prepare for and recover from terrorist strikes and disasters of all types. Such resilience results from a sustained commitment to four factors.

1. Robustness
   The ability to stay standing in the face of distance. Robustness entails good design, redundancy or substitutability, and investment in good maintenance.
2. Resourcefulness
   Skillfully managing a disaster once it unfolds. Identifying options and prioritizing what should be done to control damage and to begin mitigating it.
3. Rapid Recovery
   Resume operations as quickly as possible.
4. Review
   Learn and make changes, capture strategic advantages.

Over the past two decades, we have stopped thinking about the elements of our physical infrastructure as national security assets. In fact, increasingly it seems that we have stopped thinking about infrastructure altogether. Many of the great public works projects of the 20th century—dams and canal locks, bridges and tunnels, aquifers and aqueducts, and even the Eisenhower interstate highway system—are now old and are not aging gracefully. There are real costs associated with our neglect…When critical systems become unreliable, businesses have to invest in backup capabilities to sustain their operations. Over time, this can weaken the competitive position of companies in the international marketplace. Alternatively, a national effort to repair and upgrade these systems would bolster the attraction of investing, working and living in the United States. Company supply chains would be more efficient and reliable. Corporations could channel some of their investments in continuity-of-operations contingencies back into their core businesses. Insurance costs would be reduced.

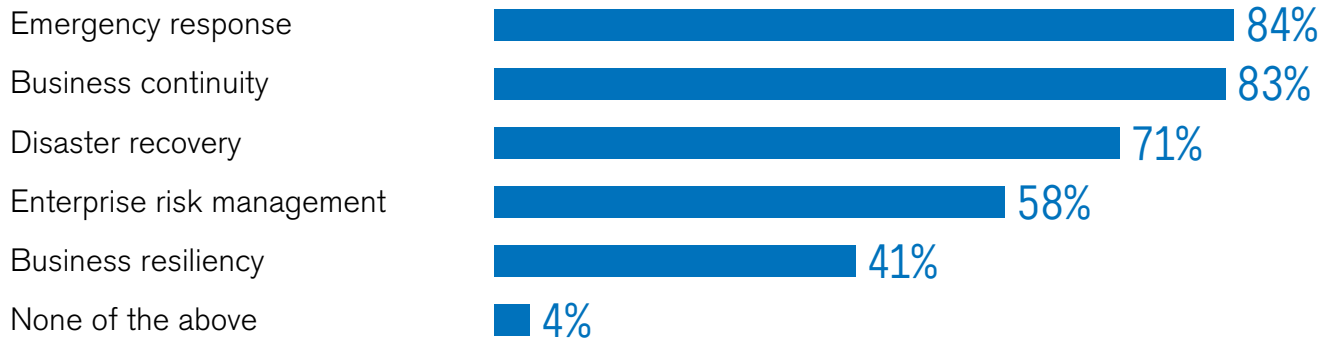
Stephen Flynn
The Edge of Disaster: Rebuilding a Resilient Nation.

2008 Business Resiliency Survey Results

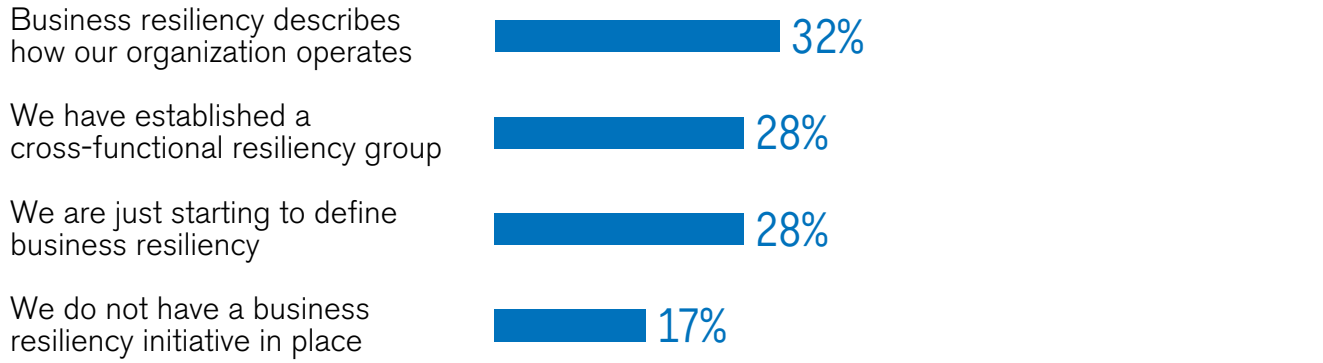
An Insider's Look at the Current State of Risk Management, Continuity and Resiliency in Multinational Organizations

Source: IJet

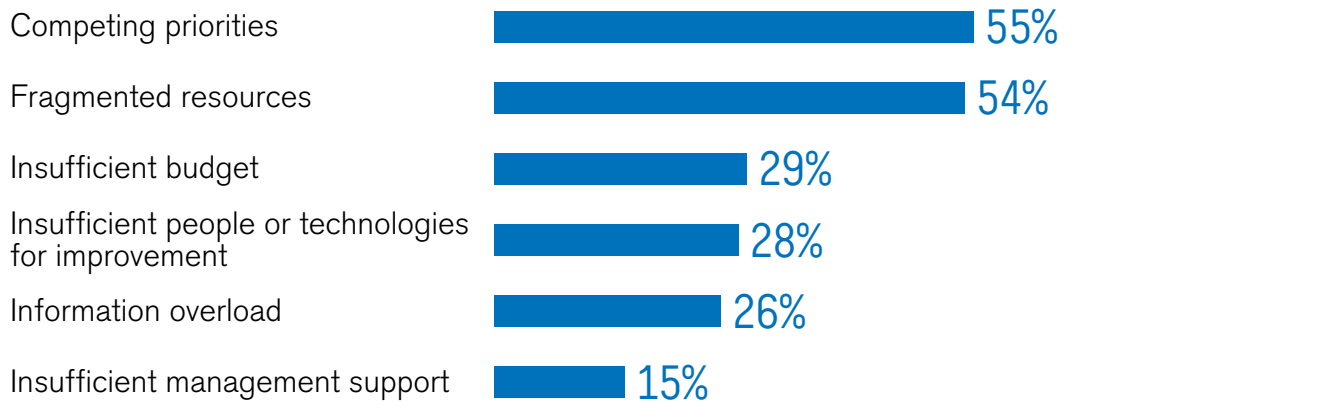
What types of plans does your organization have in place?



How would you describe your organization's approach to business resiliency?



What are the top barriers to instituting stronger risk management, continuity and resiliency plans?



Briefing Materials

Roles for Governance

"Management is doing things right; leadership is doing the right things."

Peter F. Drucker

"The only alternative to risk management is crisis management."

James Lamm

Overview

Some key surveys and studies find that directors are "in the dark" when it comes to risk management. There is general agreement that non-financial risks are poorly measured, that organizational structures for managing risk are inadequate and that boards need to take a more hands-on role in overseeing risk management processes. But there is currently no agreement on what exactly that role should be.

In the majority of companies, audit committees have primary responsibility for risk management, but they are being overwhelmed as non-financial risks (with financial reporting implications) are added to their plates. Some studies see a danger in Balkanizing risk. Others see a problem with the creation of a risk committee, which can give other board committees the perception that risk is no longer their problem.

One area that is emerging (but even less evolved) is the potential role of the audit committee to oversee internal and external audits of financial and non-financial risk management processes and to evaluate the validity of management risk rankings.

In the Dark: What Boards and Executives Don't Know About the Health of Their Businesses

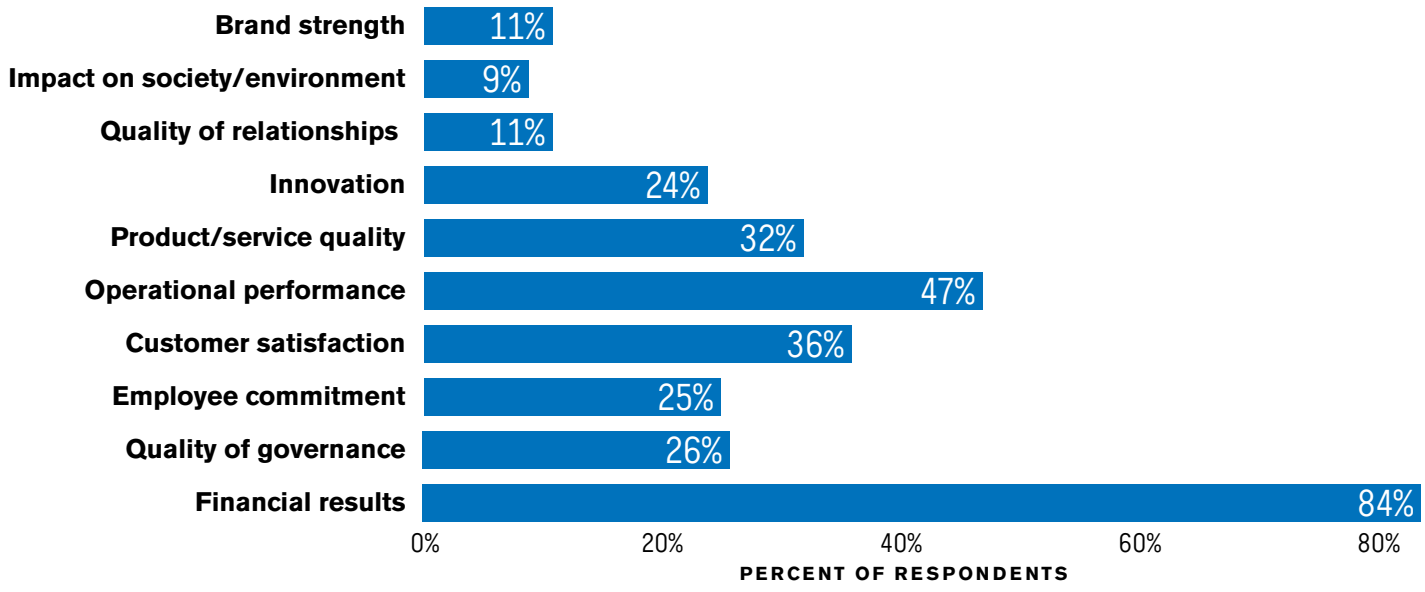
Deloitte and Economist Intelligence Unit, 2004

In a survey of 250 executives and board members, Deloitte found that the two largest barriers to effective risk governance systems were a lack of tools needed to analyze non-financial issues and a culture of skepticism that such non-financial indicators are directly related to the bottom line.

- Nearly three-quarters of executives and board directors were under pressure to measure non-financial performance indicators.
- One-third of respondents said their companies' non-financial reporting measures were excellent or good (versus an 86 percent positive response rate for financial reporting measures).
- Nearly half of respondents said non-financial reporting measures were ineffective or highly ineffective in shaping the decision-making process.

Areas in Which Board Holds Management Accountable and Offers Rewards for Good Performance

Source: Deloitte, *In the Dark II*



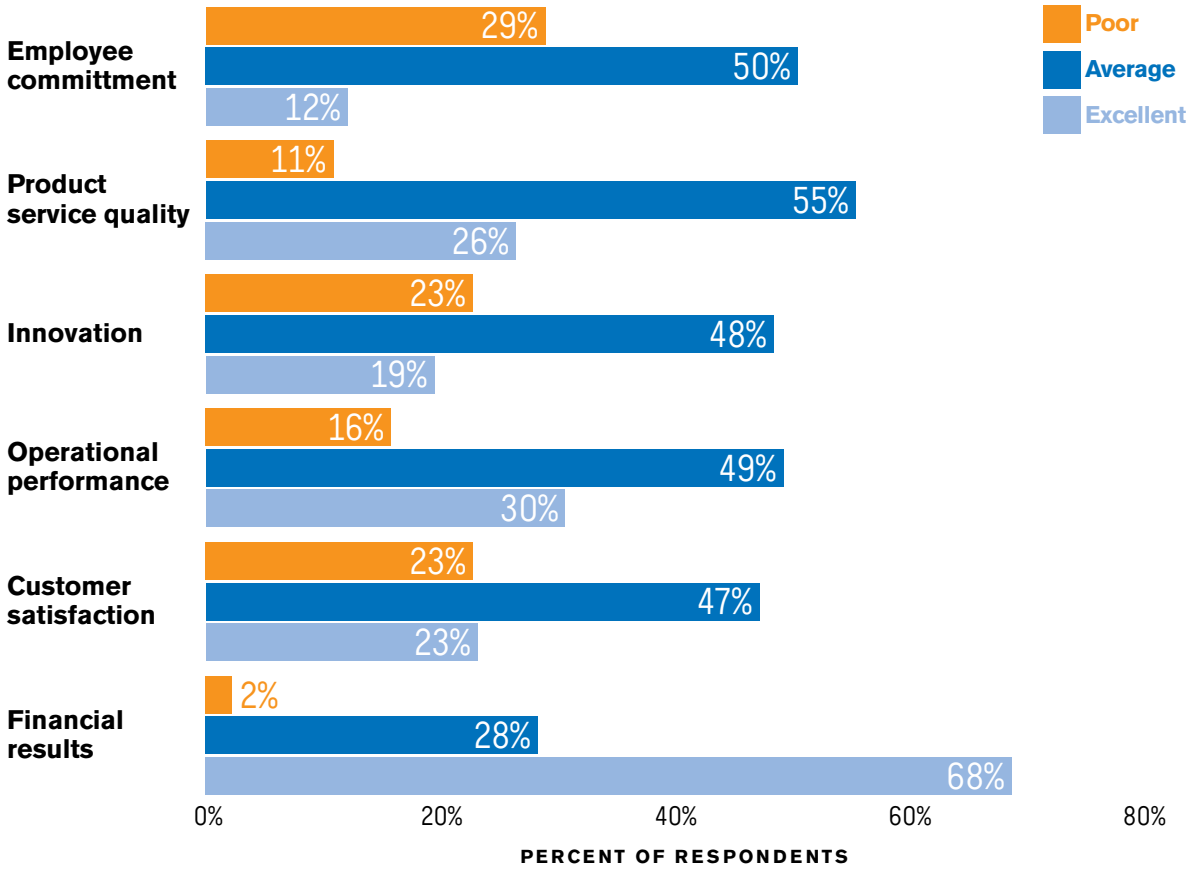
In the Dark II: What Boards and Executives Still Don't Know About the Health of Their Businesses

Deloitte and Economic Intelligence Unit, 2007

Three years later, the results were re-tested. The majority of executives perceived a growing need to better understand the underlying drivers of their performances through non-financial measurements. But, the metrics available to monitor performance remained inadequate. The study concluded that companies either did not have or were not sharing critical non-financial performance data with their boards.

Quality of Information Shared with the Board

Source: Deloitte, *In the Dark II*, 2007



Taking Risk on Board

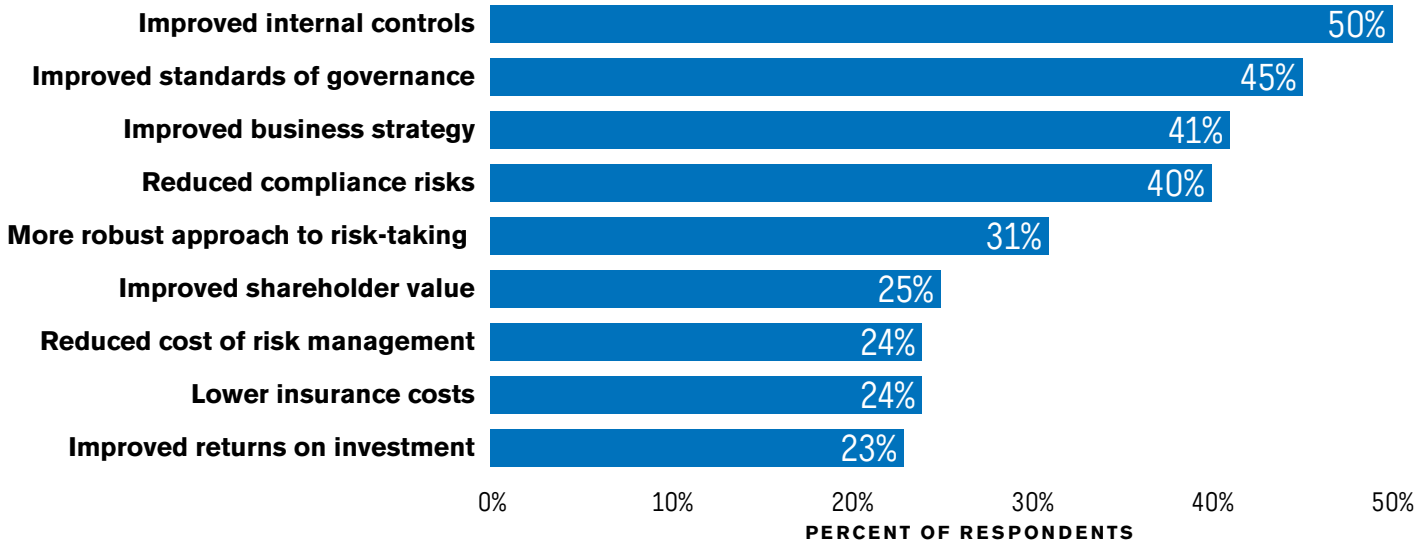
Lloyd's with the Economist Intelligence Unit, 2005

Boards are taking risk more seriously. Three years ago, just one in ten boards spent more than 10 percent of their time on formal risk management. By 2005, that number had risen to almost 40 percent. Yet, this change has not translated into greater expertise.

In the 12 months prior to the survey, one in five companies surveyed had suffered significant damage from a failure to manage risk and more than half (56 percent) had experienced at least one near miss. Ten percent of respondents reported three near misses during the past year. Adoption of risk management standards across the enterprise was limited. Only one-quarter set regular risk targets for managers, and fewer than one-third provided risk management training for managers and staff. This was viewed as symptomatic of a culture in which risk management was considered to be "someone else's job."

Positive Results Following Increased Board Responsibility for Risk Management

Source: Economist Intelligence Unit



The Risk-Intelligent Board: Viewing the World Through Risk-Colored Glasses

Steve Wagner and Maureen Errity
Deloittereview.com, Winter 2008

To meet their fiduciary responsibilities, directors must share a common vision of risk and adopt a framework to support their risk oversight activities. Unfortunately, these elements are lacking at many companies.

This is not to imply that boards are negligent when it comes to risk. Most board members make careful deliberations and bring to bear their best judgment. They summon the chief risk, strategy and audit executives along with the external auditor and others who manage exposures to risk. They listen to presentations, ask tough questions and review reports.

What is lacking is a context for understanding the issues. The board has nothing to benchmark against; directors have no processes or frameworks in place that allow them to take independent, objective views. As a result, they are left grappling with risk on an almost intuitive level, an ad hoc approach that allows issues to slip through the cracks.

Creating a risk committee is no panacea. In fact, it can be counterproductive if other board committees believe that their risk problems are solved because the risk committee is on the job.

When the risk management structure is optimized, every board committee will have risk on its agenda. Financial risk falls within the domain of the audit committee; compensation risk, the compensation committee; and succession risk, the nominating committee. Each of these committees, in turn, reports back to the full board, which processes the information to develop a full-spectrum picture of risk. And the loop is closed when the full board addresses risk issues with management on a regular basis.

Two Faces of Risk

Steve Wagner and Mark Layton
Deloittereview.com

We call the two faces of risk "rewarded risk" and "unrewarded risk".

Unrewarded risk represents what poker players call "table stakes": you've got to ante up just to get into the game. For instance, every public company in the United States must comply with payroll tax withholding laws, observe OSHA health and safety requirements and pay bills when they come due. Yet companies that perform all of these tasks in a timely and competent manner don't see their share prices surge as a result. The primary incentive for addressing these risks is value protection, not value creation.

Conversely, rewarded risk represents the strategic bets that you place during your poker game. You've assessed your hand, sussed out the competition and wagered a stack of chips with the expectation of raking in many more than you've laid out. In business, rewarded risks are those bets you make as you develop new products, enter new markets or acquire new companies. The primary motivation for taking rewarded risks is to spur value creation.

Fixate on just one side of the coin and you'll get a one-sided result. Focus on value creation (rewarded risk) to the exclusion of value protection (unrewarded risk), and you'll quickly find yourself on the slippery slope of noncompliance, litigation, reputation risk and other nastiness. Similarly, address only unrewarded risk and ignore rewarded risk, and your company may survive but will never thrive.

Global Warming: The Director's Perspective
Kevin A. Ewing
NACD-*Directors Monthly*, August 2008

Global warming presents corporate risk of the most challenging kind—dynamic, long-range and multivariable. The board's responsibility with respect to global warming is one of oversight of the executive team's efforts. Four key tasks emerge:

- Test
  Boards should continually validate the adequacy of the executive governance program;
- Communicate
  Global warming reaches into many facets of a company's operating and strategic plans and can play a cameo role in numerous presentations. Boards should consider whether these disaggregated communications will suffice;
- Advise
  Board members can, often more easily than management, import insights gained from outside sources; and
- Align
  Boards are uniquely positioned to observe the degree of alignment between the governance model being applied to global warming-related corporate risks and the strategic decision-making process as a whole.

The key is to define the oversight responsibilities of the board in relation to the responsibilities of the executive team, using traditional notions of oversight and governance to drive a disciplined corporate strategy on a complex issue.

Audit Committee Member Survey 2007-2008
KPMG

A survey of nearly 300 audit committee members of public companies revealed:

- Nine out of ten say that the audit committee has been more effective since the passage of Sarbanes-Oxley; members are confident about their oversight of "traditional financial reporting matters";
- Over half of audit committee members believe that their effectiveness is hampered by overloaded agendas, compliance activities that can detract from substantive discussion of issues and inadequate communication and coordination with the board and other standing committees; and
- Risk management is the No. 1 priority of the audit committee members, but only 28 percent are satisfied that the audit committee understands management's processes to identify and assess significant business risks. Only 21 percent are very satisfied with the information and reports they receive from management.

The Role of U.S. Corporate Boards in Enterprise Risk Management
Carolyn Kay Brancato, Matteo Tonello and Ellen Hexter, with Katharine Rose Newman
Conference Board, 2006

Key findings from the survey included:

- An increasing number of directors acknowledge that they must oversee business risk as part of their strategy-setting role. Nevertheless, most board members tend to resist excessive formalization of risk oversight processes;
- Directors believe that strategic risk rather than financial risk is their key concern;
- Most directors say they have a good or very good grasp of the risk implications of strategy, but are less likely to appreciate how the different parts of a business interact in the overall risk portfolio;

- Less than half of directors can point to the robust techniques that help them oversee risk (e.g. risk ranking), and the majority of boards do not use a ranking system as part of the risk assessment practices;
- Two-thirds of companies currently delegate risk oversight to their audit committees; and
- In 23 percent of companies, another committee shares the responsibility with the audit committee. A few, mostly financial, institutions have established separate risk committees (16 percent in the financial services area versus less than 4 percent in the non-financial services area).

A theme in the survey and interview data is that company-wide risks are too complex for the audit committee to manage exclusively, and that identifying a separate committee apart from the audit committee would most likely result in a more robust system of identifying and assessing risk management issues.

The study identifies a potential risk management structure, which can coordinate between committees principally responsible for risk and the full board. (See Governance Structure for Risk Management chart on the following page.)

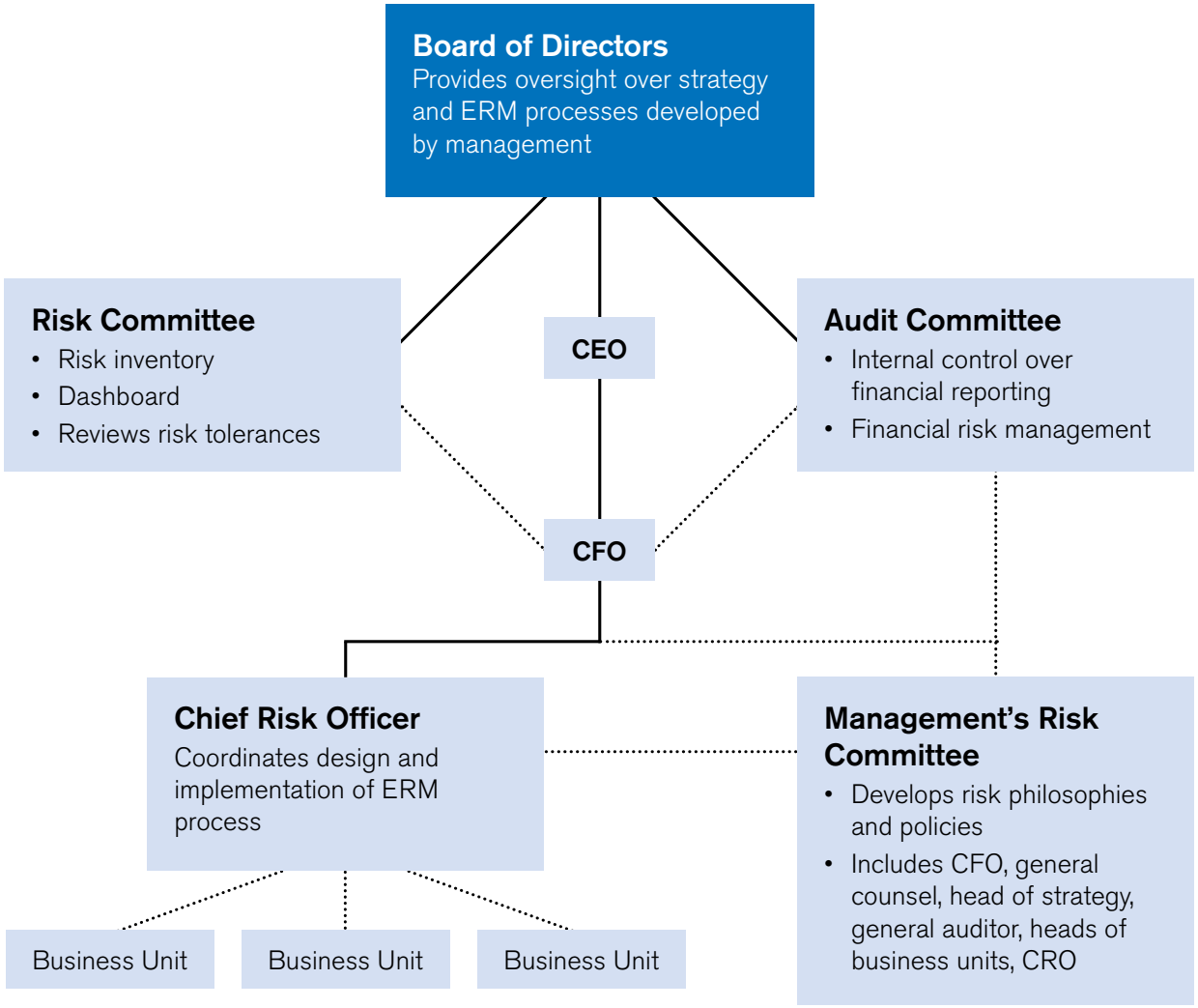
Oversight of Risk Management: Considering the Audit Committee's Role and Responsibilities
KPMG, Audit Committee Newsletter, June 2007

The oversight of risk—by audit committees, boards and other board committees—is evolving and typically lacks a clear delineation of oversight roles and responsibilities. There is no bright line that delineates oversight roles and responsibilities. On the other hand, while a committee structure can provide "specialized oversight", it may also lead to Balkanization of risk oversight activities as well as gaps in oversight.

An important role for the audit committee is to help ensure that the internal and external audit plans properly focus on internal risk controls. The audit committee should consider whether the internal and external auditors have:

- Communicated their processes for identifying and ranking the financial and non-financial reporting risks they believe may have financial reporting implications;
- Focused their audits on key areas of risk and ensured that procedures are appropriate given the potential impact and occurrence of significant risks;
- Identified the same risks that management identified, and explained any variations from identified risks or risk rankings; and
- Communicated the design and performance of planned audit procedures and demonstrated that the procedures are responsive to identified risks.

Governance Structure for Risk Management
Source: Conference Board



Briefing Materials

Recommendations for Risk Intelligence and Resilience

Overview

Much less has been written on a systems approach to creating the culture and incentive structures that reward effective risk management and resilience. There are at least three major areas to explore: management and governance; the "market movers," including ratings, insurance and audit industries; and the government by fiat, exhortation or incentive.

Roles for Management and Governance

Viewing Risk Management Strategically

Risk and Insurance Management Society, Inc. and Marsh, 2008

Strategic risk management incorporates all of the areas from traditional and progressive approaches, but adds the C-suite view of the totality of risk. The practitioner of strategic risk management views risk as something to optimize, not just to mitigate or avoid, by taking an enterprise-wide view of risk and using it to increase the company's competitive advantage. Risk is indexed against the organization itself, year after year, and against competitors. And risk management information systems and other technologies play a large role in managing risk.

Moving from Traditional to Strategic Risk Management

Source: RIMS and Marsh

Traditional Risk Management	**Progressive + Traditional Risk Management**	**Strategic + Progressive + Traditional Risk Management**
• Risk identification • Loss control • Claims analysis • Insurance and risk transfer methods	• Alternative risk financing • Business continuity • Total cost of risk • Education and communication	• Enterprise-wide risk management • Indexing of risk • Use of technology

Ultimately, the effectiveness of the enterprise risk management system will depend on the commitment of the CEO and board to implement processes that are tailored to the organization. As Rick Funston of Deloitte observes: "One size fits one."

ERM Strategies: The Good, the Bad and the Innovative

Tom Hettinger, Risk and Insurance, September 15, 2008

Companies are adopting three key strategies to manage risk on an enterprise basis:

- A risk identification mindset that pervades the company so that everyone is tuned to identify problems that could interfere with achievement of goals;
- A risk communications strategy that enables employees to share information that will uncover emerging risk possibilities; and
- Use of computer modeling and simulation to understand varying magnitudes of risk and to integrate risk information across business units and geographies.

Putting Risk in the Comfort Zone

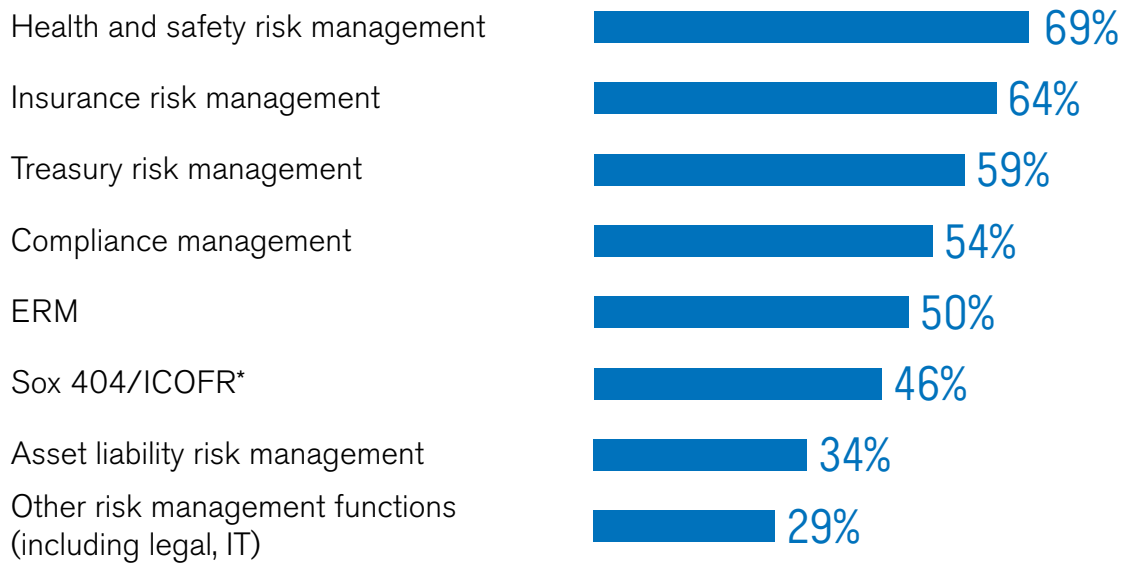
Deloitte Research, September 2008

Deloitte has identified nine principles for enterprise risk intelligence. Successful companies will:

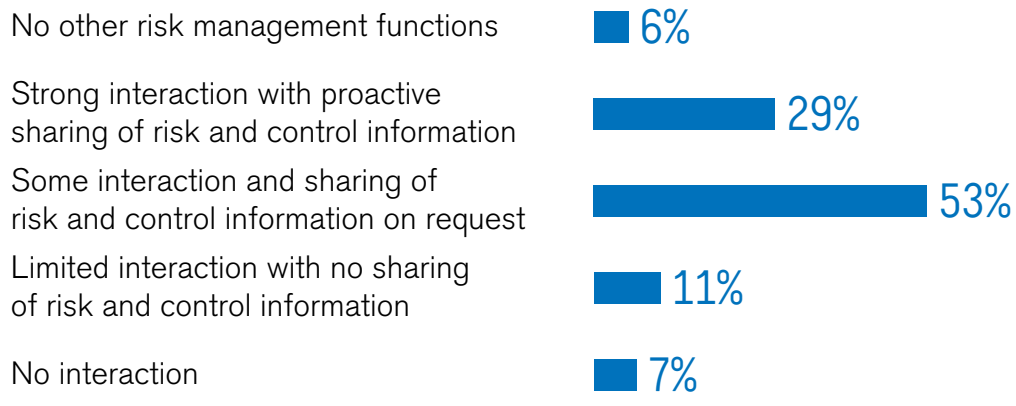
- Create a common definition for value preservation and creation;
- Establish a common risk framework supported by appropriate standards;
- Define and delineate key roles, responsibilities and authorities;
- Create a common risk management infrastructure;
- Require transparency and visibility of risk management practices for governing bodies (boards, audit committees);
- Ensure that executive management oversees design, implementation and maintenance of risk program;
- Give business units responsibility for performance and management of risk within the risk framework;
- Ensure that key functions (finance, legal, HR, tax, IT) are not only risk owners, but also support business units in risk management; and
- Have key oversight functions (audit, compliance, risk management) provide objective assurance on the effectiveness of the risk program.

Global Internal Audit Survey
Source: Ernst & Young, 2007

Companies Have Multiple Risk Management Functions…



…but Levels of Interaction Are Low



**ICOFR = Internal Controls Over Financial Reporting*

Who Needs ERM?

John J. Hampton, *Business Insurance*, July14, 2008

Who needs enterprise risk management (ERM)? My answer is, at least four people within an organization: the chief executive officer, the chief financial officer, the internal auditor and the risk manager.

If ERM means listing the 2,000 to 3,000 or so risks that face an organization, no one really needs it. An undisciplined approach to identifying risk and integrating risk mitigation into a single program will bog down after much expenditure of time and money. On the other hand, a disciplined ERM structure is just what is needed by the CEO, CFO, auditor and risk manager, among others.

The CEO and CFO seek transparency and accountability. The Sarbanes-Oxley Act requires the CEO and CFO of public companies to verify internal controls and reliability of financial statements. Rating agencies require risk programs to achieve favorable ratings on debt issues. The internal auditor is responsible for monitoring compliance with company policies and directives. The risk manager needs to present exposure to insurers and others as part of risk management and the purchase of liability coverage.

"The typical business school today is concerned with business functions, not management…The trouble with the emphasis on analysis is that it leads to an emphasis on technique or formula thinking…something that can be used in place of a brain. Technique has a place in management, but it must be used carefully and in context…not as a way of compensating for lack of experience."

Henry Mintzberg

Room for Improvement

Risks of Complacency

Towers Perrin Study Showed Business Leaders Appeared Confident in Ability to Manage Risk As Credit Crisis Loomed, Business Wire, March 13, 2008

The study showed that nine out of 10 executives believed they were as good as or better than their industry peers in managing risk and opportunity. The banking industry was the most confident about its ability to manage operational and strategic risk, and second only to the insurance industry about managing financial risk.

The study included 69 insurance industry participants, each of which was rated by S&P in terms of the firm's ERM capability—weak, adequate, strong or excellent. As part of the study, each firm's response was correlated against its S&P ERM rating. Companies with "excellent" S&P ERM ratings tended to be more risk conservative. For example, only 14 percent of the "excellent" firms were more willing to accept risk than their industry peers, versus 31 percent of other companies. These "excellent" companies also tended to be less confident about their ability to manage all risks and opportunities.

Economic Capital Models: Working Well?

Risk and Insurance, September 1, 2007

Solvency II has spurred European companies to spend a lot of time on the quantification end of risk management. They are now beginning to implement their internal economic capital models, which better reflect the value of the entire enterprise as well as valuing liabilities on a capital market basis. They are also restating their balance sheets. As they do so, some insurers are finding that, in meeting their statutory requirements, they are actually overcapitalized on an economic or capital-market valuation basis. During the first quarter of 2007, AIG says it conducted a preliminary analysis of firm-wide economic capital requirements. That analysis showed that by year end 2006, AIG had excess capital in the range of $15 billion to $20 billion.

Diffusing Risk Through Derivatives?

Risk: Keeping Ahead of the Curve, Federal Reserve Bank of Chicago, July 2008

Research shows that the aggregate use of derivative instruments—in particular rate options, interest rate futures and interest rate forwards—is associated with higher growth rates in consumer and industrial loans. Engaging in derivative activities allows banks to lessen their systematic exposure to changes in interest rates, so they can increase their lending activities without increasing total risk. It is uncertain how much banks use credit derivatives to manage risk and whether their credit derivatives positions reduce or increase systematic risk.

Roles for the Market Movers

Why don't the markets value resilience? If these are bet-the-company risks, how do analysts make buy recommendations without knowing how the company manages risk or its resilience to turbulence? With insured losses on the line, why doesn't the insurance industry play a larger role in creating a premium for resilience? Why doesn't the audit industry identify ways of verifying non-financial claims of companies? The following articles explore ways in which these market movers are beginning to move the markets.

S&P ERM Questions

Steven Dreyer, S&P Managing Director, September 2008

- How are key risks identified, updated and dealt with?
- How is risk tolerance defined and communicated?
- Who "owns" risk in the organization, and how is success measured?
- What is the board's involvement in risk management?
- How did your company respond to _____ ?

1. RATINGS AGENCIES

Enterprise Risk Management: S&P To Apply Enterprise Risk Analysis To Corporate Ratings

S&P, May 7, 2008

The ratings agency announced that it will begin to incorporate ERM into discussions with rated companies in the third quarter and begin to include commentary in ratings reports in the fourth quarter. Its proposal identifies four major analytic components:

- Firm-specific risk management culture and governance;
- Existing risk controls;
- Emerging risk preparation; and
- Strategic risk management.

A firm whose ERM program is considered weak will be missing complete controls for one or more significant risks and will have limited capabilities to identify, measure and comprehensively manage risk exposures. A firm whose ERM program is considered adequate will exhibit conventional "silo-based" risk management processes, in which risks within its business functions are well-managed, but its risk responses are not well-coordinated across business units. A company whose ERM program is rated strong will exhibit an enterprise-wide view of risks allowing for consistent identification, measurement and management of risks across business units within predetermined risk tolerances. The company will also include risk and risk management discussions in its strategic business planning efforts.

A firm rated as excellent will, in addition to those characteristics of strongly-rated companies, also exhibit risk/reward optimization behavior.

The ERM analysis will emphasize risk management culture and strategic risk management. Risk management culture includes:

- Risk-management frameworks or structures currently in use;
- Clear and defined roles for staff responsible for risk management and reporting lines;
- Internal and external risk-management communications;
- Broad risk-management policies and metrics for successful risk management; and
- The influence of risk management on budgeting and management compensation.

Strategic risk management includes:

- Management's view of the most consequential risks the firm faces, their likelihood and the potential effect on credit;
- The frequency and nature of updating the identification of these top risks;
- The influence of risk sensitivity on liability management and financing decisions; and
- The role of risk management in strategic decision making.

S&P Rolls Out ERM Review

John Cummings, *Business Finance*, May 13, 2008
businessfinancemag.com

S&P is not the only ratings agency pushing ERM. Moody's has been developing a holistic risk management rating methodology through its Enhanced Analysis Initiative. AM Best has stated that ERM will be included as an integral part of its rating process, though not as a separate rating factor.

The S&P model focuses on risk management culture and strategic risk management.

2. INSURANCE

The Risk Landscape of the Future

Swiss Re, 2004

The chief prerequisite for successful risk management is readiness to address highly unsettling questions. What would happen if the Gulf Stream were to lose strength or suddenly change course? What would it mean if nanoparticles actually penetrated the human brain directly via the olfactory nerve? What risks are created by the broad rejection of genetically modified food? The immediate purpose of discussing such scenarios is to differentiate between the possible and the impossible. In reality, the public debate about risks of the future is often dominated by equally irresponsible scaremongering and trivializing reassurance, both of which hamper any attempt at rational risk management.

Risk reduction is too often limited to efforts at reducing the probability of occurrence, not the magnitude of risk.

The world has become demonstrably safer. Since 1970, life expectancies have risen, and the number of fires and traffic accidents has declined. But despite fewer accidents, there are much higher losses per incident.

- In aviation, the number of accidents per one million takeoffs fell dramatically, but the number of fatalities per accident has doubled, and will go higher still with the introduction of 800-passenger planes.
- In rail, state of the art safety has reduced the probability of accidents, but high speed trains magnify the possible consequences as a doubling of speed means a quadrupling of the force of collision impact.
- Urban areas are growing vertically. More traffic and shopping centers are being relocated underground and, worldwide, there are 37 residential blocks higher than 200 meters and dozens more on the drawing board. Escape routes are getting longer and fires can have devastating consequences.
- Increasing dependence on power and telecommunications for economic activity has increased the potential for multibillion dollar productivity losses.

For simple linear systems, loss events can be predicted precisely if all cause and effect relationships are known. That is why it is possible to calculate how many hours an aircraft propeller can operate before becoming critically warped through the centrifugal forces that cause the metal molecules to migrate gradually to the tips of the propeller blades. For complex systems, accurate predictions are extremely difficult. The real difficulty of risk assessment does not lie in a complex system per se, but in the acceleration of changes in complex systems.

Disaster Risk Financing: Reducing the Burden on Public Budgets
Swiss Re, June 2008

Natural catastrophes are a growing certainty and a rising burden. In 2005, economic losses from natural catastrophes hit a record high, with direct financial losses of $230 billion (0.5 percent of total worldwide GDP). Despite a record insurance payout of more than $83 billion, uninsured direct losses of $150 billion had to be carried by individuals, companies and the public sector. More recently, in 2007, a total of 335 natural catastrophes led to losses of $64 billion across the globe, of which $40 billion were uninsured.

Events such as flooding, storms and heat waves place a huge burden on the public sector, which not only carries the cost of relief efforts but is also responsible for rebuilding public infrastructure. This is intensified by the fact that public entities consciously or unconsciously decide to retain risk by not insuring their infrastructure.

Although developed countries typically account for the majority of economic losses, the burden in terms of GDP is dramatically higher for developing countries. In Turkey, a single earthquake caused an economic loss of 11 percent of GDP. In the absence of widespread insurance coverage, economic losses of this magnitude can only be addressed with significant public sector or relief funding.

Traditionally, the public sector has adopted a post-event approach to disaster funding, including increasing taxes, reallocating funds from other budget items, accessing domestic and international credit and borrowing from multilateral financial institutions. Most rely on assistance from international aid.

Pursuing a post-disaster strategy has several potential disadvantages, including: diverting funds from key development projects to pay for emergency relief; paying the premium to raise new domestic debt in a credit constrained post-event market; and raising taxes which could weaken the economy further and discourage new private investments. Finally, international aid often arrives too late for immediate disaster relief.

There is value in shifting from relief to pre-event risk financing, i.e. setting up financial reserves, contingent debt agreements, insurance and alternative risk transfer solutions.

A new generation of sovereign insurance can make it easier for governments to cope with disaster. One example is the GlobeCat securitization. Launched in 2007, this solution uses financial instruments to transfer Central American earthquake risks to the capital markets. GlobeCat provides a payout based on the size of the population exposed to a specified earthquake above a threshold level. Three events of $150 million are covered in a three year period. Of this total amount, $160 million was placed in the capital markets through a catastrophe bond (that defined magnitude, location and depth) and the remainder was reinsured.

What is a Catastrophe Bond?

In essence, investors place funds in a catastrophe bond and, if a catastrophe occurs that "triggers" the bond, (each bond has a unique trigger mechanism), investors may lose some or all of the capital investment. In the case of an event, the funds are paid to the bond sponsor—an insurer, a reinsurer or corporation—to cover losses. In turn, the bond sponsors pay interest to investors for this catastrophe protection. Catastrophe bonds offer investors an attractive risk/return profile and serve to diversify portfolio risk.

Swiss Re

Crediting Preparedness

Raisch and Statler, Intercep, NYU, 2006

Apply the preparedness standard for pricing risk. The authors suggest that specific inclusion of corporate preparedness in rating and underwriting processes could deliver shareholder value. Property insurer FM Global takes the position that business interruption insurance is the last line of defense against business disruption, while the first and most important step is a holistic risk management program that includes all aspects of the facility and operation. The insurer proves the bottom-line benefits of its position by comparing the loss history of policy-holders that had implemented its loss prevention approach to those that had not.

On balance, preparedness yielded 75 percent to 85 percent lower dollar losses. For Hurricane Katrina, FM Global clients collectively spent $2.3 million to prevent losses that were estimated at $480 million. In other words, for every dollar spent on targeted preparedness measures, $208 were saved in one single major event.

3. AUDIT

The Future of Corporate Sustainability Reporting

Brian Ballou, Dan Heitger and Charles Landes
Journal of Accountancy, December 2006

Create standards for non-financial reporting areas. Using corporate sustainability reporting as an example, the authors show how audits can play an important role in non-financial reporting areas. Increasingly, social and environmental performance has become an important issue for internal and external stakeholders. A survey of investors, portfolio managers and securities analysts reported that 90 percent of those questioned said annual reports should go beyond financial and shareholder issues to include environmental sustainability and corporate governance. The most dominant reporting regulations come from the Global Reporting Initiative (GRI), which issued its first comprehensive reporting guidelines in 2002 and the G3 Reporting Framework in October 2006. As of October 2006, more than 1,000 international companies had registered with the GRI.

Although many firms have affiliated themselves with GRI standards in their corporate social responsibility reporting (CSRs), there are no commonly accepted criteria for audits of these reports. The authors conclude that as demand for reporting on corporate social responsibility and sustainability grows, so too will the role of accountants and auditors to verify the accuracy of reported information. And this may open the door to address other stakeholder demands for information on non-financial performance, such as risk management and governance.

The Right Fit: Auditing ERM Frameworks

Alexandra Psica, *Internal Auditor*, April 2008

An ERM framework is not a single policy, but an array of components within an organization that work together to manage risk over time efficiently and effectively. The auditor's task is to assess whether the sum of these components constitute a framework that is appropriate for the organization.

Establishing a Framework

Auditors should focus on the attitudes and values described in the organization's risk management policies and governance frameworks. Although auditors are not involved in establishing the framework, when they conduct an audit, they should look for evidence that the risk management practices defined in the framework are in use and operating as expected.

Assessing Risks

Auditors should check to see if the organization has a consistent risk identification process that addresses all categories of risk in its business environment. They should determine whether there is a formal risk assessment process, whether residual risk exposure is examined against established risk tolerances and whether a formal response to risk is documented and communicated.

Treating Risks

Auditors should look for action plans to manage unacceptable risks, including specific mitigation measures, time lines and owners. Key risk indicators should be identified and monitored on a regular basis by those responsible within the organization. Auditors should check for a standardized approach to managing risk information with common language and data.

Monitoring the Framework

An organization should have processes and practices that enable it to monitor the effectiveness of the ERM framework. Auditors should look for pre-established objectives and indicators that the ERM processes and framework are measured against. Auditors should assess whether there is both management oversight of the framework to ensure that the processes are working as intended and independent oversight to monitor the quality of risk management and due diligence in risk decision making.

Internal Audit Role in ERM

Source: *The role of internal audit in enterprise-wide risk management*, (power point), James Glass, director, Business Review and Audit Division, Financial Services Authority, United Kingdom

Core risk-based internal audit roles

- Giving assurance on the risk management processes
- Giving assurance that risks are correctly classified
- Evaluating risk management processes
- Evaluating reporting of key risks
- Reviewing the management of key risks

Legitimate internal audit roles with safeguards

- Giving advice on identifying and classifying risks
- Championing establishment of ERM
- Facilitating risk workshops
- Facilitating management's response to risk
- Central coordinating point for ERM
- Monitoring risks across the business
- Holistic reporting on risks
- Developing risk management strategy for board approval
- Operating the ERM framework

Roles internal audit should not undertake

- Imposing risk management processes
- Managing risks on management's behalf
- Setting risk appetite
- Taking decisions on risk responses
- Accountability for risk management
- Management assurance on risks

Global Internal Audit
Ernst & Young, 2007

Do internal audit functions have the resources to refresh annual risk assessments?

- Eighty-nine percent of respondents conduct a risk assessment to support the internal audit planning process.
- Forty-four percent of respondents update their risk assessment semi-annually, quarterly, or prior to conducting internal audits.
- Only 44 percent of respondents provide standardized training to individuals responsible for conducting a risk assessment.
- Only 43 percent of respondents present risks not covered by the internal audit plan to the audit committee.
- Only 21 percent of respondents were able to complete the prior year internal audit plan.
- Only 24 percent completed up to 80 percent of the plan.

Roles for Government Policy

Government policies can reinforce the private sector by incentivizing investments, strengthening market mechanisms that reward resilience, creating resilience standards for government contracts to leverage its own buying power, investing in risk analytic tools and computational models that improve risk assessment capabilities and information-sharing networks, and leveraging public-private partnerships that identify needs and encourage joint solutions.

Transform
Debra van Opstal, Council on Competitiveness, June 2007

The national objective is not just protection but resilience—the ability to bounce back. And the mission is not just homeland security, but economic security—the ability to resume operations and take advantage of new opportunities.

To create a more resilient economy, the government should:

Lead By Incentive

- Leverage the government's buying clout to embed resilience criteria into procurement processes and supply chains;
- Leverage the government's investments in technology to embed resilience criteria into the evaluation and selection of emerging technologies;
- Leverage market incentives more creatively; and
- Expand guidance on disclosure of non-financial material risks in SEC filings.

Create More Effective Partnerships that Reduce Cost and Risk

- Fund additional research to apply computational modeling and simulation capabilities to risk assessments;
- 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; and
- Expand the program of technology test beds that help companies test innovative security solutions without interrupting or endangering current operating systems.

Education and Training: Change the Culture

- Establish a resilience curriculum fund to which universities or other education/training providers can apply for funding to develop programs—either stand-alone or modules embedded into existing curricula; and
- Stimulate cross-disciplinary research that creates new capabilities for understanding complex systems, interactions and interdependencies.

Homeland Security 3.0

Heyman and Carafano, The Heritage Foundation and CSIS, September 18, 2008

Major areas of recommendation include: empowering a national culture of preparedness; shifting to a resilience-based strategy; expanding international cooperation throughout homeland security programs; developing a framework for domestic intelligence; and establishing national programs to improve professional development in security and public safety. With respect to risk and resilience, the report recommends that the federal government:

- Allocate financial support and other federal resources on a risk basis, not on fixed percentages. The federal government should highlight best practices, and develop and promote baseline community preparedness capabilities standards. The federal government should develop a basic risk assessment to enable communities to evaluate relative risks realistically.
- Establish a model that delineates governmental and private sector roles and responsibilities. Defeating terrorists is not the private sector's job. Government should be clear on what it expects from the private sector, as well as:
  - Define what is reasonable through clear processes and performance measures;
  - Create transparency and the means to measure performance;
  - Provide legal protections to encourage information sharing and initiative; and
  - Tailor expectations to the unique characteristics of each sector.
- Propose and fund an investment strategy to facilitate public-private partnerships more effec-tively, target national transportation trust funds by creating an independent infrastructure fund, encourage joint investment in border infrastructure, transfer federal trust funds back to the states, and focus investments on project-based financing.
- Develop leadership on global and national resiliency issues. The term "critical infrastructure" has often been used in a sloppy and overly-inclusive manner, lumping "critical" and "dangerous" into one concept. Critical assets need to be made more resilient through greater redundancy, robustness and/or decentralization, while dangerous facilities must be protected against attack.

A country risk officer, comparable to the role of a chief risk officer, is a useful model to develop an integrated perspective across the social, economic and environmental risks of a country. The country risk officer would take the lead in creating a national risk landscape, promoting the common understanding and forward-looking dialogue essential for risk prevention and adaptation measures.

Peter Forstmoser, Swiss Re

Top Ten Challenges for the Next Secretary of Homeland Security

Homeland Security Advisory Council, September 11, 2008

1. Recognize that "homeland security" is more than a single Cabinet department.
2. Inventory DHS's commitments, deadlines and work with Congress to create a rational oversight system.
3. Improve intelligence and information sharing.
4. Build a cadre of homeland security leadership through a unified system of training and education.
5. Build the R&D and acquisition process to support DHS missions.
6. Complete the work of strengthening national disaster response capabilities.
7. Lead the building of a resilient America with a:
   - Nationwide application of a "resilience metric"—time to reconstitution of everyday services;
   - All-hazards approach; and
   - Active engagement of private sector and academic sector thought leaders.
8. Balance secure borders and open doors to travelers, students and commerce.
9. Take the following steps to improve risk management and risk communications:
   - Improve risk-based approach to homeland security;
   - Establish and improve performance metrics for measuring risk and build a framework for risk-informed decision-making;
   - Consolidate existing risk management programs across components and agencies; and
   - Improve risk and crisis communications systems.
10. Improve sustainability of national homeland security efforts by strengthening the financial base and the urgency of mission focus.

Partnering With the Private Sector to Secure Critical Infrastructure

William G. Raisch, Testimony
House Homeland Security Committee, May 14, 2008

Implement legislation passed in 2007 that calls for the development of a voluntary private sector certification program for all-hazards emergency preparedness.

Government should consistently engage the private sector in the development and implementation of the program, maintain an integrated approach across relevant offices and functions, provide sustaining resources to the program, evaluate the voluntary application of the program to critical infrastructure, and help to develop education and tools to enable businesses to pursue program assessment and implementation with minimal cost and disruption.

Building a Resilient Nation: Enhancing Security, Ensuring a Strong Economy
Reform Institute, October 2008

A truly resilient nation places equal emphasis on preparedness, protection, response and recovery so that it can withstand disruptive events that it knows are inevitable irrespective of their origin.

- The next administration and Congress must refocus the nation's homeland security policy
  with resilience at its core.
- DHS needs to be a national resource—a
  clearinghouse—charged with:
  - Conducting an extensive public awareness campaign targeting U.S. industry and empha-sizing the criticality of workable business continuity plans;
  - Assisting U.S. industry in developing business continuity plans by providing templates, advice, best practices and general "help desk" like services; and
  - Taking a leadership role in the development and implementation of national, regional and local exercises with private sector interests focused on testing business continuity plans.
- Congress and the next administration need to
  refocus DHS and its customs and border protection agents on working with the private sector to more effectively identify potential threats to the global supply chain, specifically in the adoption
  of more effective screening technologies and deployment of "smart containers".

Neglected Defense

Flynn and Prieto, Council on Foreign Relations, March 2006

There are three reasons why relying on the market as the primary catalyst for critical infrastructure protection is flawed. First, security is a public good and core responsibility of government. Second, by relegating itself to "protector of last resort", Washington ends up taking a wait-and-see approach that delays the pursuit of practical security measures. Third, if private sector preparedness is simply assumed, the only way to validate that the private sector is prepared is after an attack.

To make America more secure:

- Washington needs to change its policy paradigm, which in effect tells companies to protect themselves;
- Washington must move beyond talking about information sharing with the private sector and hold government officials accountable for actually doing it;
- Congress and the administration should work closely with industry to establish security stand-ards and implement and enforce regulations where necessary, and especially where industry
  is seeking standards and regulation;
- Congress should establish targeted tax incentives to promote investments in security and resiliency in the highest risk industries;
- Congress should establish federal liability protections for companies that undertake meaningful security improvements;
- Private sector assets and capabilities should be fully integrated into more frequent exercises to respond to catastrophic events; and
- DHS should establish a federal awards program, modeled after the Baldrige Quality Award, which recognizes private sector achievement and innovation in homeland security.

Council on Competitiveness

Council Membership

GENERAL MEMBERSHIP

Michael F. Adams
University of Georgia

Robert A. Altenkirch
New Jersey Institute of Technology

Joseph E. Aoun
Northeastern University

Alain J. P. Belda
Alcoa, Inc.

Thomas R. Baruch
CMEA Ventures

Lee C. Bollinger
Columbia University

Molly Corbett Broad
American Council on Education

Richard H. Brodhead
Duke University

David L. Callender
The University of Texas, Medical Branch at Galveston

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

Judith F. Cardenas
Center for Performance Accountability, Inc.

Curtis R. Carlson
SRI International

David F. Carney
Lincoln Educational Services

John T. Casteen, III
University of Virginia

Clarence P. Cazalot, Jr.
Marathon Oil Corporation

Thomas A. Cellucci
Department of Homeland Security

Roy A. Church
Lorain County Community College

James K. Clifton
The Gallup Organization

Mary Sue Coleman
The University of Michigan

France A. Córdova
Purdue University

Michael M. Crow
Arizona State University

Ronald J. Daniels
The Johns Hopkins University

William W. Destler
Rochester Institute of Technology

Ernest J. Dianastasis
CAI

Amr ElSawy
Noblis, Inc.

Roger A. Enrico
DreamWorks Animation SKG Inc.

Alice P. Gast
Lehigh University

E. Gordon Gee
The Ohio State University

Judy Genshaft
University of South Florida

Robert B. Graybill
Nimbis Services, Inc.

Amy Gutmann
University of Pennsylvania

Patrick T. Harker
University of Delaware

William C. Harris
Science Foundation Arizona

Richard H. Herman
University of Illinois at Urbana-Champaign

John C. Hitt
University of Central Florida

Jerry MacArthur Hultin
Polytechnic Institute of NYU

Jeffrey R. Immelt
General Electric Company

Ralph Izzo
Public Service Enterprise Group Incorporated

Irwin M. Jacobs
QUALCOMM, Inc.

John I. Jenkins
University of Notre Dame

Paul G. Kimball
Sagebrush Capital, LLC

Donald R. Knauss
The Clorox Company

Robert W. Lane
Deere & Company

Lester A. Lefton
Kent State University

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

Michael A. McRobbie
Indiana University

Alan G. Merten
George Mason University

James B. Milliken
University of Nebraska

C. Daniel Mote, Jr.
University of Maryland

Eileen K. Murray
Investment Risk Management

Mark A. Nordenberg
University of Pittsburgh

Edward E. Nusbaum
Grant Thornton LLP

Thomas F. O'Neill
Sandler O'Neill + Partners, L.P.

James W. Owens
Caterpillar Inc.

Vikram S. Pandit
Citigroup Inc.

Harris Pastides
University of South Carolina

G.P. "Bud" Peterson
Georgia Institute of Technology

Peter G. Peterson
The Blackstone Group

Dominic J. Pileggi
Thomas & Betts Corporation

Rory Riggs
Balfour, LLC

John W. Rowe
Exelon Corporation

Steven B. Sample
University of Southern California

Leonard A. Schlesinger
Babson College

Carl J. Schramm
Ewing Marion Kauffman Foundation

Ivan G. Seidenberg
Verizon Communications Inc.

M. Edward Sellers
BlueCross BlueShield of South Carolina

Scott D. Sheffield
Pioneer Natural Resources Company

Jan F. Simek
The University of Tennessee

John B. Simpson
State University of New York at Buffalo

Michael P. Skarzynski
Arbitron Inc.

David J. Skorton
Cornell University

Frederick W. Smith
FedEx Corporation

Christine J. Sobek
Waubonsee Community College

Mary S. Spangler
Houston Community College

Graham B. Spanier
The Pennsylvania State University

Susan S. Stautberg
Partner Com Corporation

Charles W. Steger
Virginia Polytechnic Institute and State University

Robert J. Stevens
Lockheed Martin Corporation

Christopher Stone
SiCortex, Inc.

John A. Swainson
CA Inc.

John E. Treat
Alternative Hybrid Locomotive Technologies

Tom Uhlman
New Venture Partners LLC

Steven L. VanAusdle
Walla Walla Community College

Larry N. Vanderhoef
University of California, Davis

Jeffrey Wadsworth
Battelle Memorial Institute

Joseph L. Welch
ITC Holdings Corp.

William C. Weldon
Johnson & Johnson

Deborah Westphal
Toffler Associates

William Weyand
MSC Software Corporation

Timothy P. White
University of California, Riverside

Jack M. Wilson
The University of Massachusetts

James E. Wright
Dartmouth College

Mark S. Wrighton
Washington University in St. Louis

Henry T. Yang
University of California, Santa Barbara

Paul A. Yarossi
HNTB Holdings Ltd.

Nicholas S. Zeppos
Vanderbilt University

National Affiliates and Council Staff

NATIONAL AFFILIATES

AIGA
American Association for the Advancement of Science
American Association of Community Colleges
American Chamber of Commerce Executives
American Council on Renewable Energy
American Institute for Medical and Biological Engineering
American Mathematical Society
American Society for Engineering Education
Arizona Technology Council
Arlington Chamber of Commerce
ASME
Association of American Colleges and Universities
Association of American Universities
Association of University Related Research Parks
Ben Franklin Technology Partners
BITS, Financial Services Roundtable
COMAP, Inc
Council on Governmental Relations
Delaware Technology Park, Inc.
Detroit Renaissance Inc.
Georgia Research Alliance, Inc.
IEEE-USA
International Economic Development Council
Iowa Business Council
JumpStart Inc
National Center for Manufacturing Sciences
National Center for Women & Information Technology
NEW CAROLINA
Northwest Food Processors Innovation Productivity Center
Northeast Ohio Technology Coalition
Nuclear Energy Institute
Oak Ridge Associated Universities
Rothman Institute for Entrepreneurial Studies
SMC3
Technology CEO Council
The Bi-National Sustainability Laboratory
United Negro College Fund
United States Council for International Business
University Economic Development Association

DISTINGUISHED FELLOWS

Erich Bloch
Daniel S. Goldin
Alexander A. Karsner
Alan P. Larson
Thomas Ridge
Anthony J. Tether

SENIOR FELLOWS

Edward J. Donnelly
Lisa Guillermin Gable
Amy Kaslow

SENIOR ADVISORS

Jennifer Bond
Ronald Stowe
Denise Swink

COUNCIL SENIOR STAFF

Deborah L. Wince-Smith
President

C. Wm. Booher, Jr.
Executive Vice President, Chief Operating Officer and Treasurer

Sandy K. Baruah
Executive Vice President

Chad Evans
Senior Vice President

Cynthia R. McIntyre
Senior Vice President

Susan Rochford
Senior Vice President

Debra van Opstal
Senior Vice President and Secretary

William C. Bates
Vice President for Government Affairs

Mohamed N. Khan
Vice President for Information Services

Betsy Thurston
Vice President for Strategic Development

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 ensuring 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, DC 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 stakeholders to translate policy into action and change

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

Compete.
Council on Competitiveness