Davos-Klosters 2009

An MIT Press Journal

innovations

TECHNOLOGY | GOVERNANCE | GLOBALIZATION

Special Edition for the World Economic Forum Annual Meeting 2009

Social Innovation in a Post-Crisis World

FEATURING SCHWAB SOCIAL ENTREPRENEURS

innovations

Technology | Governance | Globalization

Special Edition for the World Economic Forum Annual Meeting 2009

About *Innovations*

***Innovations* is about entrepreneurial solutions to global challenges.**

The journal features cases authored by exceptional innovators; commentary and research from leading academics; and essays from globally recognized executives and political leaders. The journal is jointly hosted at George Mason University's School of Public Policy, Harvard's Kennedy School of Government, and MIT's Legatum Center for Development and Entrepreneurship.

mitpress.mit.edu/innovations

Philip Auerswald and Debra van Opstal

Coping with Turbulence: The Resilience Imperative

Change in the 21st century is rapid-fire and turbulent. As globalization, technological complexity, and interdependence have created new opportunities, they have also created new uncertainties. In this environment, resilience is emerging as a new and increasingly critical priority for companies and countries alike. Yet few people understand why resilience is critical—or even what it is.

WHY RESILIENCE MATTERS

Here's a simple resilience awareness test. Which of the following has the potential to disrupt business and society on a large scale: terrorist attacks, overgrown trees or leaking water? The correct answer is all of the above. The terrorism option is obvious. But, overgrown branches in Ohio were a proximate cause of a cascading power blackout across state and national borders and multiple power grids, which left 50 million people in the United States and Canada without power for several days and caused $4 billion to $6 billion in economic losses. And, in 1984, water leaking into a chemical containment vessel at the Union Carbide plant in Bhopal, India, created a cloud of toxic gas that led to the world's worst industrial disaster: it killed 3,000 people and injured 200,000.

Obvious risks are not the only ones that need attention. For business, it is not enough to plan based only on known risks—quantified and modeled under business-as-usual assumptions. For government, it is not enough to fortify against high-impact, low-probability events: the malicious terrorist attacks or natural disasters that capture popular imagination. Risks are just as likely to emanate from disruptions in global networks—for energy, communication, information, trans-

Philip Auerswald is a Founding Co-Editor of Innovations*, an Assistant Professor and Director of the Center for Science and Technology Policy at George Mason University, and a Research Associate at Harvard University's Kennedy School of Government. He is an editor of* Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability *(Cambridge University Press, 2006).*

Debra van Opstal is the Senior Vice President of Programs and Policy at the Council on Competitiveness, a Washington-based, nonprofit, nonpartisan organization whose members are CEOs, university presidents, and heads of labor unions. Before joining the council, she was the Fellow in Science and Technology and Deputy Director of the S&T program at the Center for Strategic and International Studies in Washington.

portation—that are interlocked, allowing failures to cascade across networks, borders, and societies.

Resilience is the quality that enables enterprises and societies to cope with those unexpected events that have potentially catastrophic consequences. In this essay we argue that a sustained strategic focus on resilience—one as intense as that ordinarily placed on growth—is an urgent priority for business and government at all levels worldwide.

For countries, a strategic focus on resilience means not only ensuring the reliable provision of basic services but also reducing the variations in economic opportunity that come with major societal shocks. Where sustainability (a more familiar term as applied to policy) is about managing a level of resource consumption, resilience is about managing disruptions to critical systems—physical, virtual, health, and economic. A resilient society can cope with a variety of such disruptions to critical systems with agility, speed, and resourcefulness.

Resilience is the quality that enables enterprises and societies to cope with those unexpected events that have potentially catastrophic consequences. In this essay we argue that a sustained strategic focus on resilience—one as intense as that ordinarily placed on growth—is an urgent priority for business and government at all levels worldwide.

For companies, resilience is about anticipating, managing, and responding to sudden change. As has become all too evident in recent months, a firm's shareholders and customers are not well served when a market valuation built on years of strong quarterly reports crumbles when an unanticipated hazard exposes inadequate preparedness. But resilience is not just about avoiding losses or preserve shareholder value. It is also about being poised to seize suddenly available opportunities to create value. The organization that pays attention to flexibility and adaptability—and has prepared for a spectrum of surprises—is better equipped not just mitigate disasters, but also to capitalize on such opportunities.

When it comes to understanding the resilience imperative, however, many companies fall short. This happens partly because the risk landscape has changed so dramatically in just the last decade. Global enterprises now operate quite differently from the multinationals of the last century, but their risk management processes have not kept pace. Multinational companies typically transplanted themselves as self-contained businesses on foreign shores, but global enterprises

splice different pieces of their business operations across different geographies, and network them to each other through voice and data IT systems and supply chains. That has raised the ante on network disruptions from operational downtime to a "bet the bottom line" risk.

And globalization is creating new strategic risks. The Global Risk Network at the World Economic Forum identifies strategic trends that could create significant economic losses. But are companies connecting the dots between these strategic risks and their own risk-management processes? Resilience requires companies to create innovative approaches to manage threat, risk, and change. What they need is not an improved ability to predict the future, but systems that can better adapt to turbulence and surprise. Resilience requires process innovation: disciplined, systematic, and cross-functional thinking across the organization, including its missions, operations, markets, and technical infrastructure.

When resilience fails, private-sector organizations pay a price. The problem is that their failures have far-reaching consequences for public welfare as well—regionally, nationally, and sometimes globally. Traditionally, governments have refrained from intervening in the way that companies manage risk and resilience, understanding that the markets will exact a toll. But the stakes have increased beyond anyone's expectations.

> Companies, communities and citizens create an ecosystem of resilience. Businesses cannot be resilient if the communities in which they operate and the citizens they employ are not also resilient. A company may be ready to resume operations following a disruption, but the surrounding infrastructure might not be functioning or the citizens might be psychologically unready to return to normalcy.

Countries are not much better prepared. We have just seen the failures in U.S. financial risk management cascade across sectors and trigger a global financial and credit crisis. Trillions of dollars of value in market capitalization has been lost. The entire developed world has been driven into recession, not just a growth slowdown. As a result, the Director General of the International Labor Organization (ILO) reports, world unemployment is likely to increase by 20 million over the coming year. The number of working poor living on under $1 a day could rise by some 40 million and the number at $2 a day by more than 100 million.[1]

What Business Leaders Should Know About Resilience

The rise in operational and strategic risks is outpacing traditional risk-management systems.

The past 20 years has seen a dramatic decrease in the number of stocks receiving a high-quality rating from Standard & Poor's and a dramatic increase in the number of low-quality stocks. Meanwhile, from 1993 to 2003, more than one third of Fortune 1000 companies lost at least 60% of their value in a single year.[2]

A survey by Lloyds of London and the *Economist* found that one company in five had suffered significant damage from a failure to manage risk and over half (56%) had experienced at least one near miss. Ten percent of respondents reported three near misses during the previous year.[3]

Surveys show that a preponderance of board directors and senior executives are poorly informed about emerging risks.

- In a survey of 250 executives and board members, the two largest barriers to effective risk governance systems were a lack of tools for analyzing non-financial issues and a culture of skepticism that such non-financial indicators are directly related to the bottom line.[4]
- Only one-third of respondents said their non-financial reporting measures were excellent or good.
- Nearly half of respondents said non-financial factors were ineffective or highly ineffective in informing the decision-making process.[5]

Companies tend to silo risk specialties and often fail to connect the dots between risk intelligence and strategic planning.

A study by Deloitte Research 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% 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 longstanding. 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.[6]

Most companies monitor multiple risks—from environment, health and safety to market and credit risk to compliance and IT security, but less than 30% report strong interaction between the risk silos and proactive sharing of information.[7] And, unfortunately, risk doesn't respect silos. A data breach is not just a problem for IT professionals; it can rapidly evolve into a reputation risk, a litigation risk, and a financial risk that engages the entire enterprise.

Technological risks to societies are rising as well. Although the number of accidents is dropping, the losses for each one are much higher.

- In aviation, the number of accidents per one million take-offs has fallen dramatically, but the number of fatalities per accident has doubled—and will rise higher still with 800-passenger planes.
- In rail, state-of-the-art safety has reduced the probability of accidents, but high-speed trains multiply the possible consequences because a doubling of speed means a quadrupling of collision impact.
- Urban areas are growing vertically: more traffic areas and shopping centers are relocated underground, where fires can have devastating consequences and escape routes are getting longer. Worldwide there are 37 residential blocks higher than 200 meters and dozens more on the drawing board.

To prepare for turbulence and change, governments must be ready to change the way they prepare and partner.

Global welfare now depends on the resilience of a set of complex technological systems (much of it privately owned), economic activities (much of them privately conducted), and resource utilization that affects the lives and livelihoods of people around the world.

Companies, communities and citizens create an ecosystem of resilience. Businesses cannot be resilient if the communities in which they operate and the citizens they employ are not also resilient. A company may be ready to resume operations following a disruption, but the surrounding infrastructure might not be functioning or the citizens might be psychologically unready to return to normalcy.

To prepare for turbulence and change, governments must be ready to change the way they prepare and partner. They need to reexamine the relationships and responsibilities of the public and private sectors, understanding the crucial web of mutual interest and interdependencies. And a critical new skill is required for effective policy and governance: an ability to adapt to the unexpected. But that adaptability is rarely spontaneous.

Resilience requires more than reactive responses; it reaches beyond proactive preparation. Resilient systems, enterprises, and individuals put into place the culture, training, and processes to manage change with agility and resourcefulness.

ENDOGENOUS VULNERABILITIES: A PARABLE OF THE PRESENT

Just as the industrial age showed us that environmental vulnerabilities are an economic and social reality, so the post-industrial age in which we now live is expos-

ing a different set of vulnerabilities: the endogenous security vulnerabilities of a civil society.

Private actors seeking to increase competitiveness through greater operational efficiency will normally outsource, automate, or eliminate tasks they see as peripheral to their core business competency, and they will avoid investing in equipment they see as redundant. To reduce costs, managers may seek ways to make use of external infrastructures for which others bear the cost: consider how firms use the Internet as the backbone of their internal corporate communications. They may undertake to reduce redundancy in internal systems and decrease the depths of their protective firewalls to levels consistent with "normal" levels of risk.[8] They may take other actions, including mergers and acquisitions, to realize economies of scale and scope: to improve corporate performance by embracing a wider range of functions and opportunities.

Distributed efforts to improve productive efficiency at the firm level have yielded countless improvements; together, over the past decades, these have resulted in staggering reductions in costs. Yet competitive pressures do not allow firms to make large investments aimed at reducing vulnerability to disasters that are highly unlikely and nearly impossible to predict.

The public can also be vulnerable to *endogenous events*: those whose outcome results at least partly from human actions. Hurricane Katrina is a good example. The hurricane damage was magnified first by the failure of the system of levees and barriers protecting the city of New Orleans, and second by the failure of the public officials responsible for protecting its people. For example, the communications systems collapsed and no security protocols were in place that would enable infrastructure service providers from the private sector to reach affected areas.

An *exogenous* counter-example is a meteor strike: this event is completely the result of actions beyond human control.[9] Until recently, hurricanes and other extreme weather events were similarly viewed as exogenous events and were described, in the language of faith rather than of economics, as "acts of God." But we increasingly understand that human actions affect not only the impacts of extreme events but actually the probability of their occurrence. Cumulative decisions weaken natural barriers to storm surges, place human populations in vulnerable areas, and change environmental and climate patterns on a global scale. Natural disasters are no longer acts of God; they are now a function of human choices. In all the millennia of human history, this has never happened before.

Thus the abstract concept of an *endogenous security vulnerability* is present everywhere today in the brick-and-mortar world of everyday business decision-making. Moreover, the increasing race for competitiveness and economies of scale pushes firms to develop ever-larger systems, with larger potential associated risks. Many examples exist of large-scale and/or highly connected infrastructures vulnerable to unlikely events, with severe consequences if they do occur. Athletic facilities can now hold 100,000 persons, aircraft like the new Airbus 380 can seat up to 850 passengers, and a new Royal Caribbean cruise liner that carries 6,400 vacationers. Food processing and distribution firms serve ever-increasing shares of the

national market, and power distribution networks serve a third of the nation's population. [10] In each of these examples, the quest for economies of scale induced by a highly competitive market economy has the potential to amplify the consequences of a catastrophic failure in an infrastructure system.

Ironically, the existence of endogenous vulnerabilities has now been most starkly illustrated right where we thought we had the most robust quantitative systems for managing risk: in the financial markets. A May 2007 article in *The Economist* describes the relationship between incremental innovation, growth in profitability, and increased vulnerability. Read in retrospect, it documents how the underlying risks that unraveled capital markets this past fall were hidden in plain sight for more than two years:

> [I]nvestment banks have played a crucial part in bringing about the extraordinary changes seen in the financial markets, starting in the 1980s and accelerating dramatically in the past five years. Technology and innovation have brought unprecedented breadth, depth and richness to financial instruments. According to McKinsey, a consultancy, the stock of shares and public and private debt securities held in America grew from 2.4 times GDP in 1995 to 3.3 times in 2004. In Europe the increase was even more dramatic, albeit from a lower base. These figures do not include derivatives, notional amounts of which traded privately, or "over-the-counter" securities, which had soared to $370 trillion by last June, from $258 trillion less than two years earlier, according to the Bank for International Settlements (BIS). Given such torrid growth, the markets are becoming increasingly vital to global financial stability…[11]

To be sure, private firms have a strong incentive to avoid calamities in which their actions (or inactions) are functionally related. But alignment of public and private incentives goes only as far as the scale of the smallest event that could put an end to the firm. It is precisely where the accountability of the private firm leaves off that the responsibility of the public sector picks up:

> Investment bankers themselves have a vested interest in not blowing up their firms. The biggest banks are thought to be investing hundreds of millions of dollars a year in technologies to measure risk and stress-test it. Comfortingly, regulators who scrutinize the banks' risk-weighted capital say it is stronger than ever. But capital is only one line of defense. The banks' ability to cope with liquidity crises and credit crunches is harder to gauge.
>
> Facing rapid innovations among firms in the financial sector, government officials were placed in the uncomfortable role of either impeding innovations, with the risk of undermining the prospects for longer-term growth, or permitting innovations, with the risk of exposing the public to costly outcomes.[12]

Taking risks and managing them is an investment bank's core business. Bankers believe that through their risk-taking, their industry supports entrepreneurs and hence economic growth. The trouble is that new risks are almost invariably explored before anyone has developed a good way to measure them.

> [R]egulators reckon that on balance the growth of markets has been a good thing, making the financial system safer than more traditional forms of bank lending. The trouble is that given the complexity of the new instruments and the range of clients and countries involved, they can never be absolutely sure that a monumental crisis is not brewing somewhere.[13]

A system-wide liquidity crisis is exactly the sort of failure of interdependent systems that risk models, calibrated against a business-as-usual baseline, cannot handle. Yet it is also the sort of low-probability, high-consequence event for which responsible officials in the public sector must, seemingly against all odds, seek to prepare.

SOCIAL INNOVATION AND RESILIENCE: THE NEED FOR NEW PUBLIC POLICIES

Given the risks created by endogenous vulnerabilities—be they related to financial market instability, network resilience, climate change, or high-consequence terrorist attack—governments must begin to examine the nature of the relationship with the private sector.

Key questions to consider:

- Where the public interest in outcomes is substantial, what role should the government play in minimizing citizens' exposure to risk?
- How can government initiatives aimed at addressing the public's risk exposure be designed and implemented so that they enhance, rather than inhibit, the function of the markets on which the economy depends?
- How can companies that invest in resilient operations be rewarded for their contributions to public welfare?

Markets alone cannot, and will not, correct for endogenous vulnerabilities without the engagement of government. This is because markets don't price the true value of the risk to the public caused by endogenous vulnerabilities. This is a familiar concept. In the case of environmental externalities, the price mechanism is ineffective because the good in question (clear air or clean water) is not traded. In the case of the security externalities, the absence of the relevant market is only part of the problem. The other, more severe part of the problem is that private accountability leaves off where public vulnerability picks up.

A paramount challenge to government, and governance, in the 21st century is thus to arrive at a set of policy instruments that will firmly and insistently "nudge"[14] markets toward resilience—protecting the public interest without dictating operational terms of action.

The government can affect private decision-making to reduce public vulnerabilities in three ways:

- affect relative prices and profits;
- expand technological options; and
- reinforce market incentives for change.

Affect Relative Prices and Profits

To address situations in which private actors do not take into account the public consequence of their actions, government can simply tax (or subsidize) the offending (or beneficial) activity. Taxes designed to change behavior, as opposed to taxes designed simply to raise revenue, are known as "Pigouvian" taxes, after the early 20th century English economist Arthur Cecil Pigou.[15] Some Pigouvian taxes, such as those on cigarettes, seek to limit consumption behaviors that primarily harm the consumer directly; others, such as those on gasoline and other environmental "bads," seek to limit consumption behaviors that do not harm the consumer directly but are understood to harm society. The most obvious example in public discussion today is the gas tax. With commodity prices recently in freefall and the public more aware of the negative externalities of gas consumption, the United States has a great opportunity to begin to bring the amount of its gasoline tax into line with that imposed in other developed countries. An increase in the gas tax could help finance reductions in taxes on income—which, as anyone employed will be glad to report, is a "good."

> A paramount challenge to government, and governance, in the 21st century is thus to arrive at a set of policy instruments that will firmly and insistently "nudge" markets toward resilience—protecting the public interest without dictating operational terms of action.

Pigouvian taxes like those on gasoline work because, in an otherwise stable environment, we expect that increasing the price of any existing good, service, or (notably) input into a production process will lead to a decrease in its usage. However, and importantly, the magnitude of the change in usage generated by a Pigouvian tax depends on the availability of good substitutes, as well as the overall cost share of the input. As a consequence, while policy can predictably affect behavior through a Pigouvian tax, the magnitude of the induced impact will vary substantially depending on the particulars of the situation. So, getting back to a gas

tax, a winning policy agenda involves not only reducing taxes on "goods" but also spending some significant share of the revenue to improve the quality and availability of substitutes to gasoline. The better the available substitutes, the more effective the Pigouvian tax.

Consider a second example related to societal resilience: management of vulnerabilities associated with the transport of toxic inhalation hazard (TIH) chemicals. Increasing the rail rates charged for TIH-chemical shipments may induce firms with good substitution options—for example, water treatment plants using chlorine gas—to reduce or eliminate their TIH usage, as intended. Other firms, however, may have more limited substitution options—for example, plastics manufacturers using chlorine gas. For them the increased rates will simply amount to a transfer from chemical producers to the government without any significant public benefit having been achieved, as presumably intended, through a reduction in the quantity of TIH chemical shipments.

Pigouvian taxes are likely to be even less effective in inducing changes in behavior when the good or service in question is a capital good rather than an input into production. Price is only one of the various parameters of interest to a firm contemplating the purchase of a capital good. Also of first-order importance are performance, durability, and the costs of finance. Policy can affect each of these decision-making margins in different ways. It can contribute to improved performance by setting standards. It can partly resolve uncertainty regarding performance and durability through testing and certification. Various policy mechanisms to facilitate capital investments can also encourage adoption. And, of course, the government can employ a procurement mechanism to increase volumes and reduce the costs of capital goods and other products whose adoption by industry would reduce public exposure to risk.

Thus, Pigouvian taxes are good at affecting the mix of inputs into a production process. And, in some circumstances, they may induce firms to seek entirely new approaches.

Expand Technological Options

Policy action can also influence risk reduction by increasing the range of technological options in areas that pertain to the public interest. The primary mechanism available to government along these lines is direct or indirect support of research and development.

The difference between this sort of subsidy and the Pigouvian subsidy described above is that an R&D subsidy is provided in an entirely different market from the one in which the external effect is present. For example, returning again to the transport of toxic chemicals, a Pigouvian policy might levy a surcharge on railcars containing TIH chemicals. In a technology-based approach, a government R&D program would subsidize firms that seek competitive new approaches to accomplish industrial tasks with less intensive use of TIH chemicals.

While the benefits of improved technology are evident and continued advance a necessity, a public policy strategy that emphasizes technology development alone faces at least three fundamental obstacles:

Uncertainty. Research is an inherently uncertain process. Technical solutions with desirable specifications may be achievable, but they cannot be counted on to materialize when they are needed.

Long Time Horizons. To research new technical options and bring the most beneficial among them into practice is a process that routinely requires a decade or more. Such time-frames put outcomes outside of the scope of accountability for corporate leaders, directors of federal agencies, and elected officials alike.

System Integration Challenges. Industry supply chains are large, complex technical systems whose modification can result in unintended consequences. The generic challenge of transitioning an invention into a market-ready innovation is exacerbated here by the difficulty of embedding a new innovation into these complex systems.

But government can play a positive role in aligning public and private interests by using technology collaboratories, changing procurement standards, and modeling vulnerabilities and failure paths.

*Technology Collaboratories.*The U.S. Department of Energy (DOE) has used strategic collaboration to reduce risk and encourage investment in more secure energy control systems. The public stake in and need for such systems has become increasingly obvious since 9/11. In 2001, a disgruntled employee hacked into the control system of a sewage plant in Australia, triggering a large discharge. In 2003, the Slammer worm infiltrated the operations network of a nuclear power plant and for five hours disabled a panel used to monitor the plant's safety indicators. More organized, malicious actors could have increased the toll immeasurably.

Rather than regulate a security standard, the DOE created an opportunity for companies to test security software packages in a simulated environment before deploying them. The National Scada Test Bed (NSTB) used the latest cyber attack tools and computer experts to probe the vulnerability of the systems and provide a confidential assessment and mitigation roadmap. Within a few years, more than 80% of vendors of control systems in the oil, natural gas, and power sectors had taken advantage of the opportunity.

Procurement Requirements. The government should never underestimate its ability to influence the private sector through the procurement process. In the United States, the federal government buys around $400 billion in goods and services and could leverage that purchasing power to set new standards for resilience for its vendors. In fact, many private firms have already adopted contract requirements to ensure that their supply chains are resilient. Although the federal government has traditionally supported social objectives, such as reserving percentages of procurement for affirmative action and small businesses, it has yet to exercise its market clout in requiring vendors to meet resilience standards.

Simulation and Modeling. The government could also provide access to high-performance computing systems, resident in the national laboratories, to create

more visibility into vulnerabilities for private enterprises. With better modeling and simulation capabilities, the interrelationships among different types of risk, potential failure paths, and the company's exposure to loss can be modeled and quantified—and such data might motivate CEOs and corporate boards to take action. Such models have been developed for complex engineering challenges but are equally relevant in providing insight into multiple, interacting risks in the business processes.

Reinforce Market Incentives for Change

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.

Government could reinforce these trends. It could adopt new disclosure requirements that accelerate our understanding of how companies are managing risk and change. It could incorporate more sophisticated approaches to total risk engineering in its own policies and risk-management responsibilities, and it could create new pre-event financing options that leverage commercial markets to diffuse risk.

Adopt New Disclosure Requirements. The government could reinforce these trends is 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.[16]

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 prac-

tices, 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.[17]

In contrast, some of the leading insurers and re-insurers 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% to 85% 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.[18]

> 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 to reinforce market mechanisms?

Government could incorporate the 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 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% 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.[19]

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.

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 also 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.

CONCLUSION

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.

While technology creates both quality of life benefits and competitive advantages for societies and enterprises, it also carries the potential for larger and more widespread disruptions. Rates of technology diffusion have been increasing geometrically. It took 55 years for the automobile to spread to a quarter of the country, 35 years for the telephone, 22 years for the radio, 16 years for the PC, and only 7 years for the Internet.[20] Innovation, and its rapid global diffusion, has made life easier for hundreds of millions of people and driven up productivity rates worldwide. But it has also increased the extent of disruption when the technology networks fail, and has increased the cost to companies. For example, the hourly costs of downtime for U.S. companies were estimated at $2.8 million for the energy sector, $2 million for the telecom sector, and $1.6 million for manufacturing.

Globalization both mitigates risk and creates new ones. So some companies are leveraging geography to disperse risk. Rather than creating static backup sites (which often gather dust until a disruption occurs), they are creating shadow seats in each of their locations and cross-training employees in different geographies to ensure that critical functions continue in case of an emergency. On the other hand, the diffusion of interconnected operations also increases a company's exposure to infrastructure disruptions—in the systems of transportation, communications, and information that otherwise enable the enterprise to operate seamlessly across different geographies. Suddenly we see the rapid spread of other phenomena: from contagious diseases among employees traveling between sites, to widespread geopolitical instabilities and terrorism.

Private risk failures now have the potential to create public sector catastrophes. Risk failures in the public sector—for example, a failure of public health systems to contain outbreaks of contagious diseases or manage the availability of vaccines—can cascade into the private sector's ability to rely on its workforce and manage its workflow.

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.

---

1. ILO, Media and Public Information, October 20, 2000. Reference Number: ILO/08/45 http://www.ilo.org/global/About_the_ILO/Media_and_public_information/Press_releases/lang—en/WCMS_099529/index.htm .

2. Adrian Slywotzky and John Drzik, "Countering the Biggest Risk of All," *Harvard Business Review*, April 2005.
3. Lloyd's of London with the Economist Intelligence Unit, *Taking Risk On Board*, 2005, p. 6.
4. Deloitte Research and Economist Intelligence Unit, *In the Dark: What Boards and Executives Don't Know About the Health of their Business*, 2004, p. 4.
5. Deloitte Research and Economist Intelligence Unit, *In the Dark II: What Many Boards and Executives Still Don't Know About the Health of their Business*, 2007, p. 2.
6. Deloitte & Touche, *Disarming the Value Killers*, 2005, p. 1.
7. Ernst & Young, *Global Internal Audit Survey*, 2007, p. 5.
8. This section draws from Philip Auerswald, Lewis Branscomb, Erwann Michel-Kerjan, and Todd La Porte (eds.), *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, Cambridge, U.K.: Cambridge University Press, 2006. Many additional examples are cited in National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, Washington DC: National Academies Press, 2002.
9. For discussion a variety of catastrophes, including one that could be caused by a large meteor hitting the earth, see Richard Posner, *Catastrophe: Risk and Response*, Oxford U.K.: Oxford University Press, 2004. The meteor case illustrates a catastrophe in which human actions could mitigate impact, but not the probability of an event occurring.
10. For further discussion see e.g. Swiss Re, *The Risk Landscape of the Future,* 2004.
http://www.swissre.com/pws/research%20publications/risk%20and%20expertise/risk%20perception/the%20risk%20landscape%20of%20the%20future.html
11. *The Economist*, "The alchemists of finance," May 18, 2007, special section pp. 3-6.
12. Ibid.
13. Ibid.
14. See Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness.* New Haven, CT: Yale University Press, 2008.
15. Former Chairman of the Council of Economic Advisors Greg Mankiw is among the founding members of a recently constituted "Pigou Club" advocating for higher Pigouvian taxes.
16. Debra van Opstal, *Transform*, Council on Competitiveness, 2007, p. 41.
17. 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.
18. William Raisch and Matt Statler, *Crediting Preparedness*, International Center for Enterprise Preparedness, NYU, August 2, 2006. http://www.nyu.edu/intercep/research/
19. Swiss Re, *Disaster Risk Financing: Reducing the Burden on Public Budgets.* Swiss Re, June 2008, p. 2.
20. Council on Competitiveness, *Innovate America,* 2005, p. 37.

innovations
Technology | Governance | Globalization

Support for Production of the *Innovations*
Special Edition for the World Economic Forum Annual Meeting 2009
Provided by the **Schwab Foundation for Social Entrepreneurship**

INNOVATIONS IS JOINTLY HOSTED BY

GEORGE MASON UNIVERSITY
School of Public Policy
Center for Science and Technology Policy

HARVARD UNIVERSITY
Kennedy School of Government
Belfer Center for Science and International Affairs

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
Legatum Center for Development and Entrepreneurship

with assistance from

The Lemelson Foundation

The Ewing Marion Kauffman Foundation

The Ash Institute for Democratic Governance and Innovation, Harvard University

The Center for Global Studies, George Mason University

mitpress.mit.edu/innovations
editors@innovationsjournal.net