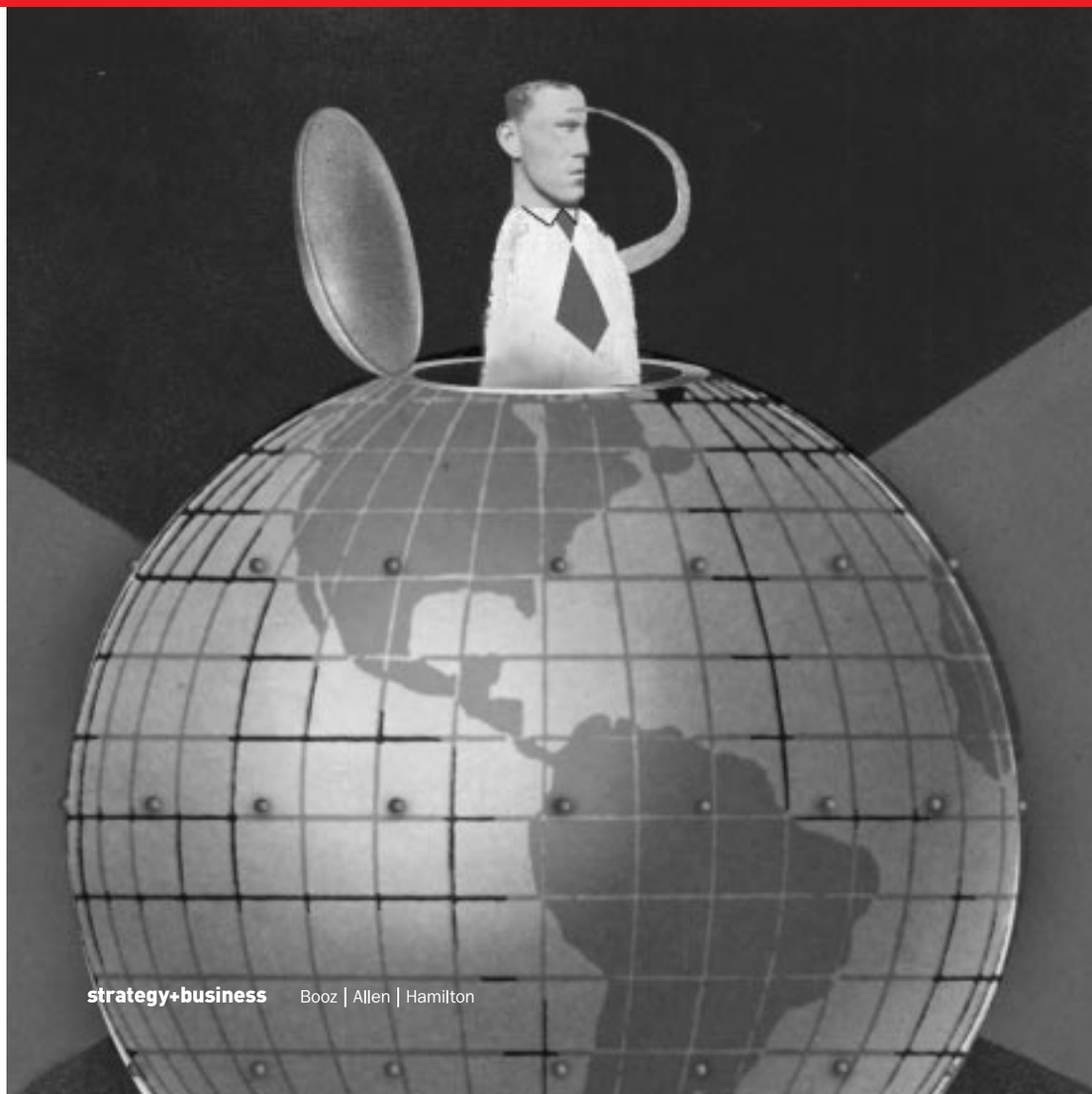
A strategy+business Reader

Enterprise Resilience: Risk and Security in the Networked World

strategy+business Booz | Allen | Hamilton

Enterprise Resilience: Risk and Security in the Networked World

A strategy+business Reader



strategy+business Booz | Allen | Hamilton

Booz Allen Hamilton Worldwide Offices

Abu Dhabi
Charles El-Hage
971-2-6-270882

Amsterdam
Peter Mensing
31-20-504-1900

Atlanta
Joe Garner
404-659-3600

Bangkok
Tim Jackson
66-2-653-2255

Beirut
Charles El-Hage
961-1-336433

Berlin
René Perillieux
49-30-88705-0

Bogotá
Jaime Maldonado
57-1-313-0202

Boston
John Harris
617-428-4400

Brisbane
Tim Jackson
61-7-3230-6400

Buenos Aires
Alejandro Stengel
54-1-14-131-0400

Caracas
José Gregorio Baquero
58-212-285-3522

Chicago
Gary Ahlquist
312-346-1900

Cleveland
Les Moeller
216-696-1900

Colorado Springs
Glen Bruels
719-597-8005

Copenhagen
Kenny Palmberg
45-3393-36-73

Dallas
Tim Blansett
214-746-6500

Düsseldorf
Thomas Kuenstner
49-211-38900

Frankfurt
Rainer Bernnat
49-69-97167-0

Göteborg
Bengt Johannesson
46-31-725-93-00

Helsinki
Kari Iloranta
358-9-61-54-600

Hong Kong
Reg Boudinot
852-2634-1878

Houston
Joe Quoyeser
713-650-4100

Jakarta
Ian Buchanan
6221-577-0077

Lexington Park
Neil Gillespie
301-862-3110

London
Peter Bertone
44-20-7393-3333

Los Angeles
Tom Hansson
310-297-2100

Madrid
Mercedes Mostajo
34-91-5220606

Malmö
Ingemar Bengtson
46-40-690-31-00

McLean
Martin J. Bollinger
703-902-3800

Melbourne
Tim Jackson
61-3-9221-1900

Mexico City
Alonso Martinez
52-55-9178-4200

Miami
Alonso Martinez
305-670-8050

Milan
Enrico Strada
39-02-72-50-91

Munich
Richard Hauser
49-89-54525-0

New York
David Knott
212-697-1900

Oslo
Haakon Bjertnaes
47-23-11-39-00

Paris
Panos Cavoulacos
33-1-44-34-3131

Philadelphia
Molly Finn
267-330-7900

Rio de Janeiro
Paolo Pigorini
55-21-2237-8400

Rome
Fernando Napolitano
39-06-69-20-73-1

San Diego
Foster Rich
619-725-6500

San Francisco
Bruce Pasternack
415-391-1900

Santiago
Alejandro Stengel
562-445-5100

São Paulo
Letícia Costa
55-11-5501-6200

Seoul
Jong Chang
82-2-2170-7500

Stockholm
Kenny Palmberg
46-8-506-190-00

Sydney
Tim Jackson
61-2-9321-1900

Tampa
Joe Garner
813-281-4900

Tokyo
Eric Spiegel
81-3-3436-8600

Vienna
Helmut Meier
43-1-518-22-900

Warsaw
Reg Boudinot
48-22-630-6301

Wellington
Tim Jackson
64-4-915-7777

Zurich
Jens Schäedler
41-1-20-64-05-0

Enterprise Resilience: Risk and Security in the Networked World

Edited by Randall Rothenberg

with an introduction by R. James Woolsey

A strategy+business Reader

Copyright © 2003 by Booz Allen Hamilton Inc.
All rights reserved.

No reproduction is permitted in whole or part without written permission from Booz Allen Hamilton Inc. For permissions requests, contact Mark Duer by e-mail at duer_mark@strategy-business.com.

Visit Booz Allen Hamilton online at www.boozallen.com

Visit strategy+business online at www.strategy-business.com

Increase your intellectual capital by subscribing to strategy+business. To subscribe for one year (four issues), visit www.strategy-business.com or call toll-free 877 829 9108 (outside the U.S., call 850 682 7644).

Design by Opto Design
Cover art by David Plunkert

Contents

Introduction

By R. James Woolsey

VICE PRESIDENT, BOOZ ALLEN HAMILTON
FORMER U.S. DIRECTOR OF CENTRAL INTELLIGENCE

September 11, 2001 was a wake-up call to companies and governments around the globe that the world had changed. But it would be a mistake to assume that the terrorist attacks on the World Trade Center and the Pentagon were the causes of the change.

Rather, those assaults were another in a long line of indications — others include the rapid rise and fall of the dot-coms, the corporate governance crisis precipitated by the collapses of Enron and WorldCom, and the increasingly rapid pace of chief executive turnover at the world's largest companies — that firms, governments, and economies have grown increasingly interdependent.

Interdependence — the implicit reliance on entities outside the borders of your own organization or otherwise free from your direct control — is the most salient influence on contemporary organizations. Even before the Internet, the speed of development of communications technologies and the globalization of financial markets were hastening the breakdown of both bounded national markets and vertically integrated companies. Today, with the Internet casting an electronic web over the world, the borders of the enterprise have grown quite porous. One's neighbor, whether in an industry value chain or an economic trading bloc, is both a potential partner and a possible competitor — or perhaps both, simultaneously, hence the rise of such concepts as "coopetition" (for synchronous cooperation and competition), which were unknown during our more structured, and comfortable, past.

Permeable boundaries have a brutally dark side to them, of course. The rise of a disaggregated terrorist infrastructure, organized not as a command-and-control hierarchy but as affiliated networks within networks, shows the terrible damage that can be wrought by a handful of villains with a grievance and access to ever more available tools of destruction.

Substitute greed for grievance, and you see how readily severe financial damage can be inflicted on a company by secondary or tertiary parties consumed only by their own interests. A lone trader improperly dealing in complex derivatives destroyed the U.K.'s Barings Bank, the world's oldest merchant bank. Andersen, perhaps the world's leading name in accountancy, was pushed to insolvency by the loss of credibility the institution suffered because of actions taken by a group in a single office. Global information markets are quick to punish reputations; global capital markets are equally quick to move money away from the injured.

Leaders might well shrug their shoulders and argue that little can be done to guard against terrorism or willful impropriety. But interdependence subjects organizations to spiraling harm from otherwise normal risks. The loss of a key supplier by a company in a competitive marketplace can force an unprepared organization to exit that market — as has happened in the European telecommunications equipment industry. Unanticipated external disruptions can hinder an entire sector's ability to manage its costs and inventories, as happened to U.S. companies dependent on West Coast ports, which were shut by a punishing strike in late 2002.

In this environment of economic uncertainty, waning shareholder confidence, and terrorism, organizations must focus more on building more resilient business and operating models to minimize the impact of unforeseen shocks. Indeed, "enterprise resilience" is likely to become the new benchmark for organizations seeking to maintain and improve the confidence of their stakeholders.

For many organizations, particularly industrial companies, the size and nature of potential disruptions to earnings drivers are often not understood. Extended enterprises have complex and networked supply and demand chains that can have hidden failure points. Geopolitical changes can have significant effects on markets and suppliers. Brand strength, manufacturing processes, financial leverage, and alliances and joint ventures are just a few of the other earnings drivers that face risks not effectively identified or quantified by traditional risk management approaches.

Choosing the right resiliency strategy requires understanding vulnerabilities, mitigation options, and economic trade-offs. The mitigation of risks to company earnings drivers — or, in the case of nonprofit institutions and government bodies, the risks to the core mission — is accomplished in various ways, from the development of better business continuity and crisis management plans to the implementation of fundamental changes in the business models and supply chain strategy. Supply chain models, for example, can be modified by adjusting the balance between "just in time" delivery and "just in case" inventory; by creating redundancy in supply sources; by developing multiple logistics plans for ports, carriers, and border entry points; or in numerous other ways. On the demand side, firms can foster resilience by identifying possible revenue shortfalls, determining in advance what to

do about them, crafting revenue-diversification strategies — and understanding how to stabilize profitability when revenues do fall.

Booz Allen Hamilton has been a leader in promoting the need for and showing the path toward resilience. In 2001, Booz Allen, the world's leading strategy and technology consulting firm for government and commercial enterprises, created a new practice in Global Assurance/Enterprise Resilience. In calling together our experts from various functional practices — including information assurance, supply chain management, infrastructure assurance, information technology, war-gaming, strategy, and business continuity — as well as numerous industry specialists, our goal was to help individual clients (as well as entire sectors) become more resilient. Part of that guidance is contained in the pages that follow. This book collects some of the research reports and thought pieces published by Booz Allen from 2000 through 2003 in the quarterly journal *strategy+business* and elsewhere. Several of the pieces are by senior Booz Allen consultants; some are written by distinguished academics or journalists. All reflect our desire to help organizations reconnoiter their increasingly interdependent environments.

The articles include:

- Security and Strategy in the Age of Discontinuity: A Management Framework for the Post-9/11 World, by Ralph W. Shrader and Mike McConnell. Published in January 2002, this article, by Booz Allen's chairman and CEO and the former director of the U.S. National Security Agency, outlines the challenges interdependence presents for public and private sector organizations.
- Network Theory's New Math, by Michael Schrage. The codirector of the "eMarkets Initiative" at the Massachusetts Institute of Technology's Media Lab and a senior advisor to the MIT Security Studies program, Mr. Schrage provides an introduction to the burgeoning field of network dynamics.
- Karen Stephenson's Quantum Theory of Trust, by Art Kleiner. This piece, by a noted management historian, profiles a leading, maverick social network theorist, whose research has been used by such private companies as IBM and Hewlett-Packard, and has helped the U.S. Defense Department understand Al Qaeda's network.
- Enterprise Resilience: Managing Risk in the Networked Economy, by Randy Starr, Jim Newfrock, and Michael Delurey. This piece, by three senior Booz Allen executives, describes how organizations can begin to identify their earnings drivers and develop a more robust resilience posture.
- Beyond Utopia: The Realist's Guide to Supply Chain Management, by Keith Oliver, Anne Chung, and Nick Samanich. A trio of operations specialists outline the problems created by infusing increasing amounts of data into faster-moving supply chains, and the human solutions to these difficulties.
- Supply Chain Surprises, by Ed Frey, Steve Nied, and Barry Jaruzelski. Three Booz Allen supply chain specialists identify how one category of supply chain shocks — off-balance-sheet inventory — can upend a company's P&L, and show what firms can do to circumvent such liabilities.
- The New Balance Between Risk and Control, by Ralph W. Shrader. Booz Allen's chairman and CEO makes the case for leaders to maintain a tolerance for risk, but to ensure reasoned oversight via participatory management.
- From New Economy to Siege Economy: Globalization, Foreign Policy, and the CEO Agenda, by Jeffrey E. Garten. The dean of the Yale School of Management, and a former U.S. Undersecretary of Commerce for International Trade, provides a roadmap for the chief executives of global companies for understanding their roles in an interdependent economy.
- The Fortune at the Bottom of the Pyramid, by C.K. Prahalad and Stuart L. Hart. Distinguished strategy professors from, respectively, the University of Michigan Business School and the University of North Carolina's Kenan-Flagler Business School show how multinational companies can prosper by serving low-income markets and bringing sustainable prosperity to the aspiring poor.
- Bioterrorism: Improving Preparedness and Response, by Gary Ahlquist and Heather Burns, and Port Security War Game: Implications for U.S. Supply Chains, by Mark Gerencser, Jim Weinberg, and Don Vincent, are reports from strategic simulations, each involving multiple companies and government organizations, held in 2002. Each provides understanding of the role public–private sector relationships play in strengthening public and enterprise resilience.

We do not claim that these articles are the last word on security or resilience. We hope, though, that they will stimulate your thinking — and perhaps lead your organization to becoming more secure and resilient.

R. James Woolsey
McLean, Virginia
April 11, 2003

About the Authors

GARY AHLQUIST (ahlquist_gary@bah.com) is a senior vice president of Booz Allen Hamilton, based in Chicago. He specializes in the strategy-driven transformation of insurance companies, health plans, and health providers. In his 21 years with the firm, he has worked with clients on strategy, e-business, organization, and transformation programs.

HEATHER BURNS (burns_heather@bah.com) is a vice president of Booz Allen Hamilton, based in McLean, Va. She specializes in business development and service delivery efforts in program development, program management, systems development, information management technology, public outreach and information access, performance evaluation, and litigation support.

ANNE CHUNG, a former principal with Booz Allen Hamilton, specializes in operations strategy, supply chain management, and Internet-enabled operations.

MICHAEL DELUREY (delurey_mike@bah.com) is a principal with Booz Allen Hamilton in Virginia. He specializes in strategic planning, policy analysis, and policy development for government clients with a focus on complex network analysis and critical infrastructure protection.

ED FREY (frey_ed@bah.com) is a vice president with Booz Allen Hamilton in San Francisco. He focuses on operations strategy, manufacturing, and supply chain transformation.

JEFFREY E. GARTEN (Jeffrey.Garten@Yale.edu) is dean of the Yale School of Management. He was the undersecretary of commerce for international trade in the first Clinton administration and, before that, a managing director of the Blackstone Group and Lehman Brothers. A monthly columnist for *BusinessWeek*, he is also the author of *The Mind of the CEO* (Perseus Books/Basic Books, 2001).

MARK GERENCSER (gerencser_mark@bah.com) is a senior vice president of Booz Allen Hamilton, based in McLean, Va. He specializes in helping clients achieve enterprise resilience to gain a competitive advantage, maintain business continuity, and protect and increase shareholder value. In his 20 years with the firm, he has worked with the Department of Defense, the U.S. intelligence community, and such private sector industries as health care, aerospace and defense, high technology, and media.

STUART L. HART (slhart@unc.edu) is the professor of strategic management, Sarah Graham Kenan Distinguished Scholar, and codirector of the Center for Sustainable Enterprise at the University of North Carolina's Kenan–Flagler Business School.

BARRY JARUZELSKI (jaruzelski_barry@bah.com) is a vice president with Booz Allen Hamilton in New York. He concentrates on corporate strategy and organizational transformation for companies in the high-tech industry.

ART KLEINER (art@well.com) is the "Culture & Change" columnist and a regular contributor of "The Creative Mind" profiles for *strategy+business*. He teaches at New York University's Interactive Telecommunications Program. His Web site is www.well.com/user/art. Mr. Kleiner is the author of *The Age of Heretics* (Doubleday, 1996); his next book, *Who Really Matters*, will be published by Doubleday Currency in August 2003.

MIKE MCCONNELL (mcconnell_jm@bah.com) is a vice president with Booz Allen Hamilton and the former director of the National Security Agency.

JIM NEWFROCK (newfrock_jim@bah.com) is a senior director and treasurer with Booz Allen Hamilton in New Jersey. He is responsible for global risk management at the firm and specializes in the interplay of business strategy and enterprise risk.

STEVE NIED (nied_stephen@bah.com) is a principal with Booz Allen Hamilton in Chicago. He specializes in operations and performance improvement in the telecommunications and electronics industries.

KEITH OLIVER (oliver_keith@bah.com) is a senior partner in Booz Allen Hamilton's London office. He heads the firm's Global Operations Practice and has specialized in supply chain management for more than 30 years.

C.K. PRAHALAD (cprahalad@aol.com) is the Harvey C. Fruehauf Professor of Business Administration at the University of Michigan Business School, Ann Arbor. He is also the founder and chairman of Praja Inc., a pioneer company in interactive event experiences, based in San Diego, Calif.

NICK SAMANICH (samanich_nicholas@bah.com), a vice president in Booz Allen Hamilton's Cleveland office, focuses on e-business, supply chain, and information systems architectures as a member of the firm's Information Technology Practice.

MICHAEL SCHRAGE (schrage@media.mit.edu) is a codirector of the Massachusetts Institute of Technology's Media Lab's eMarkets Initiative and a senior adviser to the MIT Security Studies program. Mr. Schrage is the author of *Serious Play: How the World's Best Companies Simulate to Innovate* (Harvard Business School Press, 1999).

RALPH W. SHRADER (shrader_ralph@bah.com) is the chairman and chief executive officer of Booz Allen Hamilton, the international strategy and technology consulting firm.

RANDY STARR (starr_randy@bah.com) is a principal in Booz Allen Hamilton's New York office. He specializes in combining business and technology strategy with market insights to implement growth strategies and new business models.

DON VINCENT (vincent_don@bah.com) is a vice president of Booz Allen Hamilton, based in Falls Church, Va. He specializes in counterterrorism, consequence management, NBC Defense, and survivability. He has over 25 years of experience in management, testing, research, and development programs for infrastructure assurance and protection regarding weapons of mass destruction, for clients across the federal government.

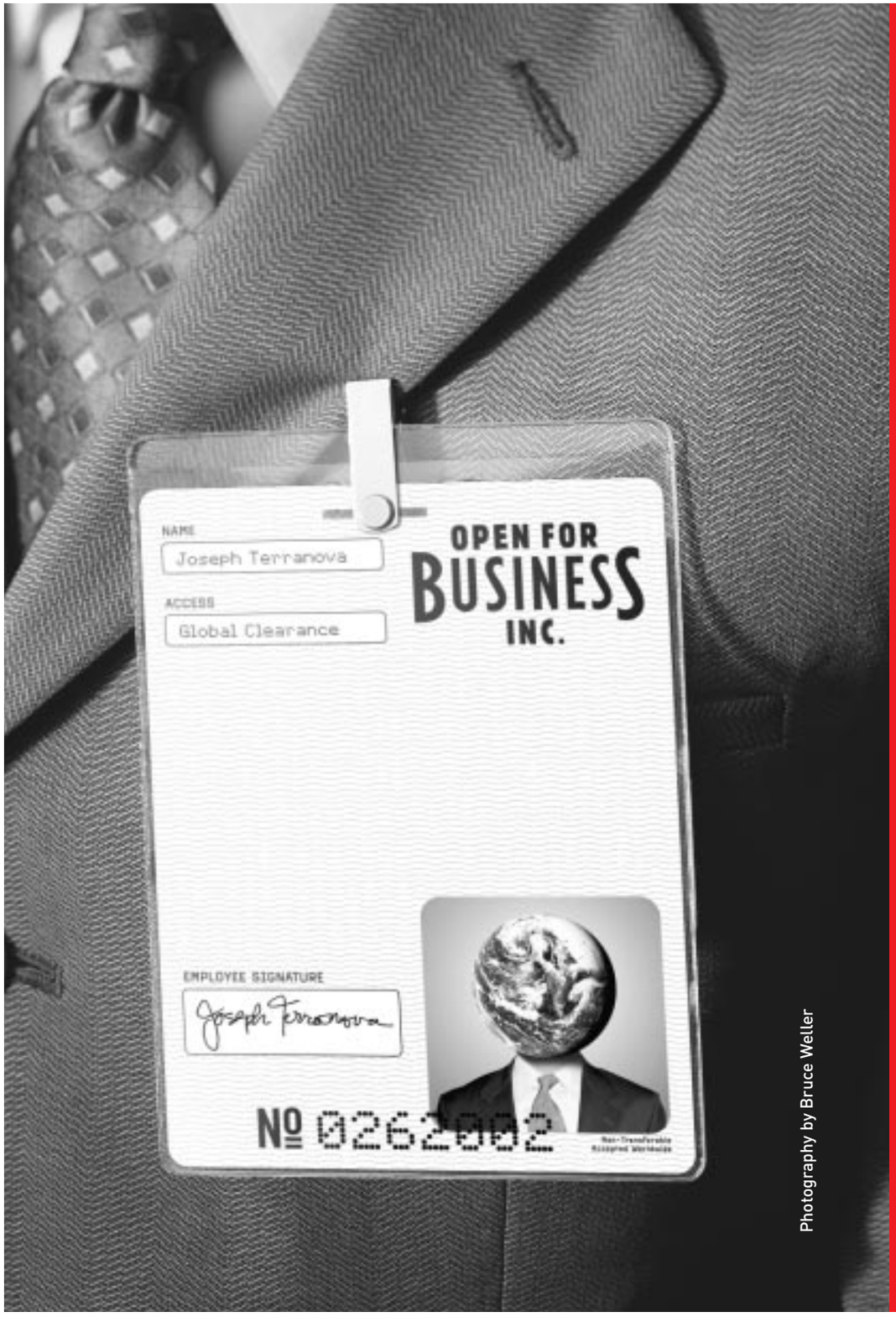
JIM WEINBERG (weinberg_jim@bah.com) is a senior vice president of Booz Allen Hamilton, based in Chicago. He assists companies in step-change improvement in operations performance through implementing new operating models and technologies. Mr. Weinberg is a coleader of Booz Allen's Enterprise Resilience practice, which is forging new frameworks for managing risk in today's dynamic and network-centric business environment.

Understanding the Networked World

Security and Strategy in the Age of Discontinuity:
A Management Framework for the Post-9/11 World
By Ralph W. Shrader and Mike McConnell
First published in *strategy+business*, First Quarter 2002

Network Theory's New Math
By Michael Schrage
First published in *strategy+business*, Fourth Quarter 2002

Karen Stephenson's Quantum Theory of Trust
By Art Kleiner
First published in *strategy+business*, Fourth Quarter 2002



Photography by Bruce Weller

Security and Strategy in the Age of Discontinuity: A Management Framework for the Post-9/11 World

Security and Strategy in the Age of Discontinuity: A Management Framework for the Post-9/11 World

by Ralph W. Shrader and Mike McConnell

Since the end of World War II, the dominant trends in Western society have been toward greater openness and greater networking among individuals, institutions, and nations. From the telephone to the Internet, from Standard Oil to the airlines' Star Alliance, from the Berlin Wall to the European Union, these trends are interdependent and have combined to increase freedom and economic growth among the countries, companies, and people that have been their beneficiaries.

The terrorists who attacked the United States and its allies, from without and within, have shown that there is a fine line between openness and exposure. Their goal is manifestly to turn a strength into a weakness. "Terrorists want to turn the openness of the global economy against itself," President George W. Bush told executives attending the Asia–Pacific Economic Cooperation forum in Shanghai last October. Their primary weapon is not civilian transportation, or invisible microbes, or any of the other bruited weapons of postmodern warfare. Rather, their weapon is fear.

In the past, people relegated the task of banishing fear to their governments. To this day, we equate leadership in times of crisis with the soothing words and bold programs of Franklin D. Roosevelt, who, on the eve of World War II, identified freedom from fear (together with freedom of expression, freedom to worship, and freedom from want) as one of the "Four Freedoms" that underpin the good society.

One of the hallmarks of the networked world is that governments now have less ability to drive progress — or reduce fear — on their own. Instead, eliminating terror and the threat it poses to the open society has become the task of both the public and the private sector. Leaders of corporations must assume a role unfamiliar to them during the past quarter-century of growing peace and greater prosperity: Alongside government and military leaders, they must strive within their own environs to evict fear, maintain openness, and sustain economic growth.

This may seem a daunting task, particularly to corporate executives stretched to the limits by the challenge of contending with a recession. In fact, the best-managed firms are capable of reducing the fear that has descended on them and their people, and can sustain the open networks necessary for their prosperity. For well-managed firms are already proficient at dealing with discontinuity, one of the most critical tasks a business faces today.

Discontinuities are the unanticipated events that can suddenly shift the landscape in an industry or for a company, requiring an immediate response either to mitigate loss or to capture opportunity. Peter F. Drucker has identified four major sources of discontinuity: the explosion of new technologies, the globalization of the economy, the growth of pluralism, and the spread of knowledge. All industries have faced these discontinuities in one form or another. The pharmaceuticals industry is subject to sudden product withdrawals and intellectual property decisions. Automobile manufacturers have had to cope with environmental regulation. Fast-food manufacturers grapple with protests by overseas activists. Financial-services firms contend with online disintermediation. In each industry, the successful companies are those that anticipate, and create adaptive mechanisms to contend with, discontinuity — the companies that, in effect, limit the sources of organizational, structural, and strategic fear.

The events of September 11 did not signal a change in the nature of the discontinuities that people, businesses, and nations face; indeed, the Al Qaeda terrorists might be viewed as an offspring of the specific discontinuities Professor Drucker identified 30 years ago. But by shutting down the largest economy in the world, deepening a worldwide recession, prompting large companies toward bankruptcy, and forcing the imminent restructuring of entire industries, the fallout from September 11 demonstrated that the severity of such discontinuities can be broader and deeper than we had previously understood. Companies that lost no employees, physical assets, or capabilities nonetheless lost revenues, market share, or value as a result of the attacks.

Moreover, the attacks demonstrated a vulnerability to "interdependence risk" — a new kind of discontinuity for most companies in most industries. Bound intimately to the globalization of communications, finance, trade, and corporate activity, as well as to the deregulation and privatization of supporting infrastructures, interdependence risk is the potential for ostensibly small events — a trader improperly covering derivatives trades, a rogue computer hacker, a fire in a supplier's factory — to spiral rapidly into a company-threatening crisis.

It is easy to be fatalistic after terrible events like those of September 11, and to

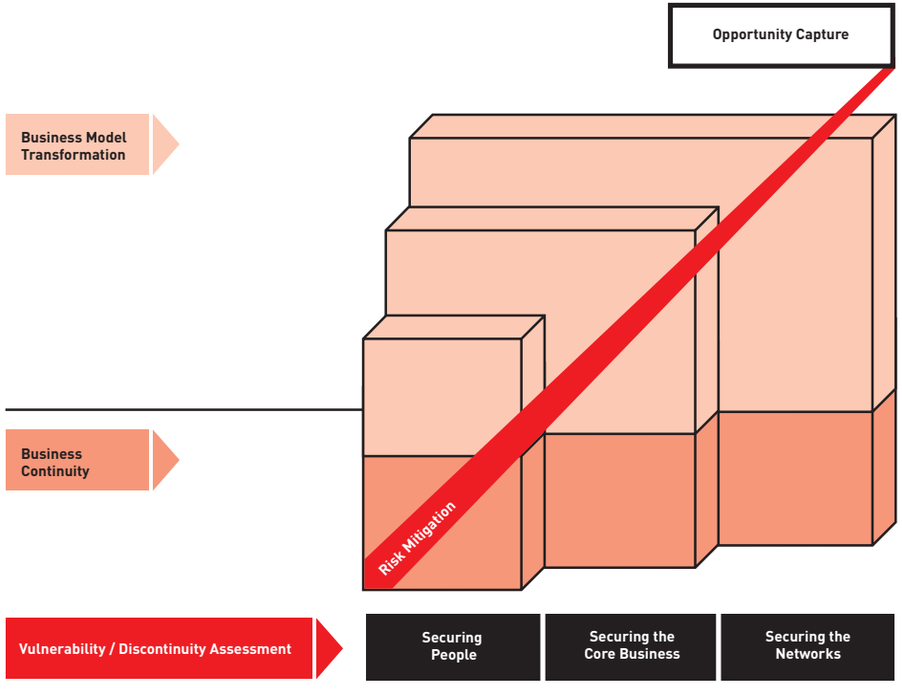
assume that there is no way to prepare — or to presume that government will step in, leaving business to face the consequences later. But pragmatic leaders will not wait for the next assault or for legislative action. We believe it is possible to protect ourselves against even the seemingly brutal discontinuities we now face. Protecting the company in this way involves far more than installing appropriate technologies, buying the right insurance policies, protecting data networks, and guarding critical infrastructure: It requires the integration of organizational security and corporate strategy. Indeed, by assimilating security and strategy, firms can not only lessen their risk exposure, but also secure opportunity, thus maintaining business resiliency, which we define as the combination of continuity and conditions for growth.

To create business resiliency, CEOs must frame a security regimen around three primary goals, which naturally build upon one another (see Exhibit 1):

• first, *securing people* — reducing the vulnerability of the men and women in the company and the fear that vulnerability generates;

• second, *securing the core business* — ensuring continuity by protecting critical owned operations and facilities, to accommodate and adapt to traditional events as well as new kinds of discontinuities;

Exhibit 1: **Strategic Security Management Framework**



• third, *securing the networks* — preserving the open information systems, supplier links, alliances, customer relationships, knowledge communities, and other components of the organization's extended ecosystem that are necessary to the functioning and growth of the modern corporation and the economies it comprises.

Underlying this enterprise-based examination of the firm's needs and prospects is a fourth requirement: a reengagement with government at all levels. Our business leaders must work closely with state and federal legislators to make certain that the security of the microeconomies they guide complements the broader measures undertaken by government, while also guaranteeing that public policy does not sacrifice openness on the altar of security, to the detriment of the economic advancement of society.

In each stage of this framework, there is both a need for risk mitigation and an opportunity for value capture, which will differ among industries and for individual companies in those industries. Furthermore, a firm must recognize that each stage has both an immediate goal — ensuring business continuity — and a longer-term objective: to examine and implement a business-model transformation, if analysis determines its necessity.

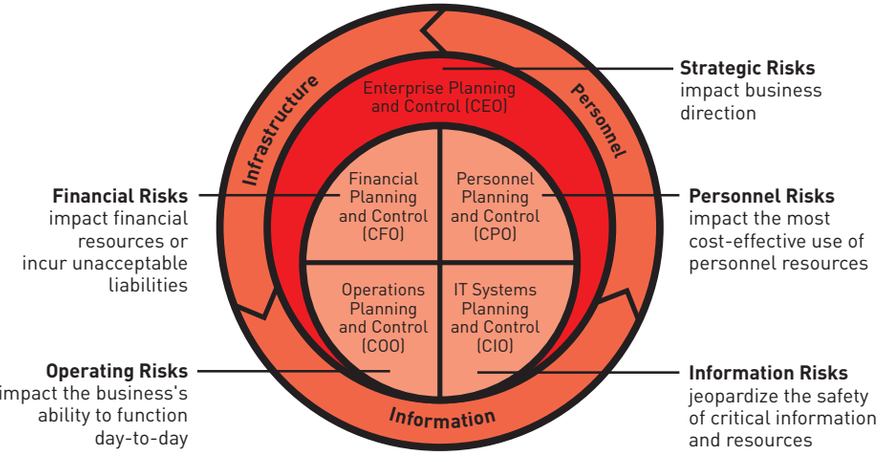
In this article, we will elaborate on this framework and the rationale for its adoption and realization. The goal is a state we call "strategic security" — security achieved in an open environment and within the context of a corporate strategy designed to facilitate growth and profitability.

Securing People

Perhaps the most salient lesson during the months that have followed the terrorist attacks on the World Trade Center and the Pentagon and the anthrax assaults that closed the Congress is that our nation's icons of freedom and prosperity also present a rich suite of targets for an elusive set of enemies. Various kinds of security threats have always existed, and some may become more prevalent over time as small-group terrorist activity spreads. But the life-changing consequence of September 11 is the perception of vulnerability in the homeland that the United States never appreciated before.

Fear for one's own safety can quite palpably cut the personal links that are the tangible essence of open economic networks. "The basest of all things is to be afraid," William Faulkner said when he accepted the Nobel Prize in 1950, at the dawn of the Cold War and amid the threat of nuclear annihilation. With threats more fragmented than they were at that time — and with interdependence risks prompting fears that few employees ever entertained before — today, strategic security must begin with freedom from fear in the work space itself.

Exhibit 2: **Integrated Risk Assurance for the Core Business**



Growing numbers of organizations have engaged in risk-mitigation exercises to address the increasing threat to their personnel. Oil companies and other firms operating in hostile countries have maintained protected compounds and transported employees to and from facilities in armored vehicles. After a spate of bombings at its domestic facilities in the late 1980s, the International Business Machines Corporation (IBM) created crisis management teams at every one of its sites in every region. These teams now train weekly and link closely to local law enforcement. From an operational point of view, they help institutionalize the company's rapid and orderly response to threats or attacks; from a personnel perspective, their presence is a regular reminder of the company's commitment to the safety and security of its people.

In a world that has grown increasingly and unfortunately violent in recent years, total risk avoidance is not a viable option: The costs would be too high, and clearly people are willing to accept some risk, or else no one would drive a car or open a piece of unfamiliar mail. Moreover, different individuals have different levels of risk tolerance and allow for adjustments in their own market value relative to the particular type of risks that they bear.

But the perception of risk is clearly undergoing a shift. Prompted by media coverage of workplace violence, harassment, environmental illnesses, and the recent air disasters and anthrax attacks, employee insecurity is rising. The implications for recruitment, retention, and productivity are real.

By having high safety standards in place, organizations increase the possibility of self-selection, so that the right kinds of people will still be attracted to the firm and remain willing to be deployed where they are needed. If a company cannot close the gap between risk and protection, it needs to rethink its strategy and assess whether it should operate in a particular environment or determine if alternatives are available. (We at Booz Allen Hamilton have closed offices when we determined we could not adequately protect employees.)

Corporate management will also need to scrutinize anew the balance between efficiency and risk. For example, companies for years have put up with the productivity deterioration associated with rampant air travel, on the theory that face-to-face meetings are crucial for maintaining internal cultures and external relationships. With the added reluctance of employees to fly in today's environment, the opportunity cost embedded in business travel may, for some companies, simply be too high, particularly after the economy recovers and working conditions again become a point of competitive advantage in attracting and retaining talent.

Securing the Core Business

One step beyond securing its people, the company has a responsibility to protect and maintain the continuity of the core business — the systems, facilities, infrastructure, and processes within the reach and control of senior management. Broadly speaking, core-business risks fall into five categories: strategic risks, operating risks, financial risks, information risks, and the previously referenced personnel risks. In most companies, these management areas are currently overseen by several senior executives, necessitating an integrated approach to security planning, under the aegis of the CEO, to make certain that all risks to the business are addressed. (See Exhibit 2.)

Although core-business protection is also largely an exercise in risk identification, prioritization, and mitigation, opportunities for value capture increase as one moves from people to businesses to networks. Done properly, and marketed effectively, an investment in appropriate levels of security can help differentiate a product or service, or enhance a company's operational effectiveness versus that of its competitors. Embedding security within the organization — effectively hardwiring it into operations, in much the same way supply chain management is today — can transform security from a burden into an enabler.

During the 1990s, about a decade after the Tylenol-tampering scare first alerted the American public to the reality of smaller-scale domestic terrorism, Procter & Gamble Company dedicated one-eighth of its research and development staff — nearly 1,000 people, of whom 250 were Ph.D. scientists — to product and packaging safety. The R&D team developed innovations such as the Safety SquEase child-resistant cap, which provided the company's Aleve analgesic with a distinct selling point at its launch. P&G subsequently sold its stake in Aleve, but Safety SquEase has been adapted for use with other P&G products.

"Safety requirements are not niceties that we incorporate simply to increase product appeal. Rather, they are corporate mandates, a nonnegotiable part of every project," a P&G executive told a "Safety Sells" conference sponsored by the U.S. Consumer Product Safety Commission in 1995.

Operationalizing strategic security in that way — building it into core processes, budgeting cycles, and strategic planning, rather than bolting it on — can give a company an advantage over slower-moving competitors. That was a central lesson of Y2K mania. Some companies built the costs of Y2K preparations into ongoing information technology budgets and were able to seamlessly revamp aging technology systems, reducing their exposure to supply chain disruptions. This better, faster, more robust market presence saved them billions in extraordinary expenses incurred by laggards.

As in the mid-'90s, companies should focus much of their short- and medium-term strategic security planning on the firm's supporting infrastructures, for it is on these systems — their operations, safety, and assurance — that business resiliency relies. The Bank of New York Company had two clearing systems with different telephone and power supplies in place on September 11, but both were in Lower Manhattan and were disabled after the attacks. The Wall Street firm Morgan Stanley Dean Witter & Company is now planning to build a second trading floor within 35 miles of its Midtown Manhattan headquarters. The backup facility, which could be elsewhere in Manhattan or in the suburbs, would not rely on the same power grid or telephone switching system as the principal office.

Fully securing business operations against any kind of attack clearly is not a realistic consideration for CEOs. However, there are some basic steps companies can take to protect their critical infrastructures. These steps are:

- Integrate all aspects of security — physical and personnel security and information assurance — across the enterprise and appoint a senior manager to control security integration and management company-wide.
- Get in touch with local, state, and federal government offices with security responsibilities that affect business and establish working partnerships to inform your risk assessments and build in a private sector input to new government plans and regulations.
- Study the company's disaster recovery plan and reassess its operating environments in light of potential new threats to business security. Develop and exercise a new disaster recovery plan and update the company-wide security program if necessary.
- Understand the risk/reward payoff for security options and sequence the rollout of a new security program to address the worst risks first.
- Review and update, review and update, repeat as necessary. The threat environ-

Understanding War Games:
A Tool for Vulnerability/Discontinuity Assessment

For many years, Booz Allen Hamilton has used strategic simulations to analyze conflict situations — from conducting "share wars" to predicting which technologies will prevail in the marketplace. Teams of players representing opposing forces, methods, or ideologies compete against each other within a defined scenario.

Simulations, also known as war games, get at things that people don't know they know, and the collective experience of the participants exposes solutions that are not apparent on the surface. The ramifications of decisions can be tested over time, and teams are able to assess the effects of a certain move after an opponent has countered with moves of its own, and then go back and make adjustments to strategy. The revised strategy can then be applied in the real world.

The threat of terrorism, as well as less-dramatic but also worrisome risks, such as internal theft of intellectual property, can be modeled using a simulation tailored to the circumstances. There is no standard way to conduct a simulation. Indeed, a simulation that tries to do everything will achieve nothing, so it's critical to establish an objective and customize rules that will lead to achieving it.

AlliedSignal Inc., for example, used a simulation to help it decide to bid for a contract to produce avionics technology — an engagement that it initially thought would not be lucrative enough to develop. In a simulation, a rival team used the knowledge it gained in producing the technology for the low-margin contract to win a much bigger piece of business that was up for grabs a few years later. Caterpillar Inc. used a competitive simulation to break the truck market into several segments represented by teams of experienced executives who, in effect, did not know how much they knew about what the marketplace wanted until they matched wits against one another.

Assessing vulnerability is not a new application for war-gaming, but it has taken on heightened significance following the attacks of September 11.

Corporations around the world have beefed up security, run evacuation drills, clarified chains of command, and reviewed procedures for everything from handling mail to reporting suspicious people. Credit Suisse First Boston, for example, instituted Project Safe House, drawing on representatives from several departments to review, recommend, and implement changes to the company's safety procedures. Beyond tactical responses, firms need to reassess the role of security within the corporate mission.

In particular, the threat of terrorism has reawakened many industries to supply chain vulnerabilities. Supply chain disruptions are nothing new, of course, but just-in-time production has led to thin margins for error. The General Motors Corporation was a victim of just-in-time delivery in 1996 when an 18-day strike by workers at two factories that supplied brakes idled 177,000 workers at 26 assembly plants, reducing quarterly earnings by $900 million.

Labor disputes certainly are more predictable than terrorism. But the effect of either kind of disruption can cripple an enterprise. That's one of the reasons that many businesses now find the need to build a response mechanism that operates every bit as efficiently as the military. Since military strategists anticipate being hit and plan for supply-line disruptions, robustness traditionally gets the nod over efficiency in the military.

Strategic simulations could help CEOs determine the proper balance between just-in-time production and resiliency, especially now that the peacetime arguments for efficiency over robustness are no longer relevant. War-gaming between different management teams can answer questions that not long ago seemed unimaginable: What would the effect on earnings be if a company stockpiled three weeks of supply measured against a precipitous drop in its stock price should a crisis disrupt production? Are there innovative ways of creating these reserves besides just paying for them outright?

A move that looks simple on the surface often proves to be wrong-minded when it's put through the discipline of a simulation. Pushing a particular lever may get the desired outcome, but it may also lead to other unanticipated effects. Corporate war-gaming helps bring these outcomes to light.

—R.W.S. and M.M.

ment, defensive tools, and a company's operations are constantly changing. Today's plan could be tomorrow's recipe for disaster.

Securing the Networks

Information attack — activities that could include outright theft of competitive intelligence, exploitation of sensitive data, disruption of an organization's network infrastructure, or destruction of valuable information — could represent a far more serious threat to some companies than physical attack, especially in the United States, where large-scale adoption of Internet-based communications and commerce systems has made companies and government agencies the world's most vulnerable. Paradoxically, the dispersed character of the Internet, designed to create an information system able to withstand a massive attack on its physical infrastructure, actually makes it and its users extremely vulnerable to cyber-attack, because the Net treats all users as privileged insiders. Hence the increasing frequency of denial-of-service attacks, computer viruses, and worms capable of crippling large companies, often for days at a time.

As the growing prevalence of information attack attests, in an economy of globally open networks, no organization is an island. Each is exposed to the vulnerabilities of the participants in its network, whether those participants are a company's own employees — or even the employees of a supplier's supplier. Senior executives must understand how the company can be affected by attacks aimed not at the enterprise itself, but at its larger community — related business sectors and their partners' own infrastructures and networks. Ford Motor Company was not attacked by Al Qaeda in September, but supply disruptions caused by government efforts to prevent future attacks cost the automotive company $30 million, as trucks bearing parts idled at the Canadian border. Thus was interdependence risk suddenly made real. Protecting the network, therefore, goes beyond safeguarding telecommunications infrastructure: It means negotiating secure policies and practices in all of the organization's critical relationships — in those associations where alliance partners can influence assets without having full ownership.

Securing against discontinuities in the extended network is no longer a foreign concept among senior executives. About six years ago, IBM created a Mission Relocations process, which facilitates the shift of manufacturing operations around the globe within 90 days. This capability has already saved the company millions of dollars by enabling it to move operations to more tax-favorable countries. It also allowed IBM to move production of chips used by the defense industry rapidly from Germany to the United States following the September 11 attacks.

But understanding the need for resilience within the extended network is still not routinized at most companies. Far from it: In pursuing basic outsourcing strategies during the past decade, most companies have sought largely to optimize efficiency at the cost of robustness. Risk has largely been excluded from the equation, catching many companies short of product at crucial times. This kind of network hazard has only grown with globalization, as companies have sought to take advantage of the increasing sophistication of overseas production by accepting extended lead times and reduced flexibility in return for lower costs.

The peril for the unprepared can be profound — as can the opportunity for ready competitors. Consider the differing responses of the Nokia Corporation of Finland and Telefon AB L.M. Ericsson of Sweden when a fire at a Koninklijke Philips Electronics NV semiconductor plant in New Mexico disrupted their supplies of chips. Nokia officials noticed a hiccup in the product flow even before Philips informed the company of the problem, and had its chief supply troubleshooter on the case immediately. Within two weeks, a team of 30 Nokia officials had fanned out over Europe, Asia, and the U.S. to patch together a solution. They redesigned chips, accelerated a project to boost production, and used the company's clout to get more chips from other suppliers. Ericsson, with fewer safeguards built into its supply network, moved more slowly and came up millions of chips short of the supply needed for a key new product. Nokia gained three share points. Ericsson lost the same, and ultimately exited the handset market.

It is critical that companies explore the discontinuity potential not only in their inner core of suppliers, but among their suppliers' suppliers as well. The Toyota Motor Corporation, one of the leading practitioners of just-in-time inventory, nearly had to stop production of its Sequoia sport utility vehicle in its Princeton, Ind., plant after the September 11 massacre: One of its own suppliers, Continental Teves Inc., was waiting for steering sensors, normally air-freighted from another company in Germany, but planes were grounded. Toyota has since worked with its suppliers to make sure they receive critical components on time. Continental Teves now has the German-made sensors shipped by boat and maintains a two-week, rather than a one-week, inventory. Such moves add inventory costs for the supplier, and as yet it is not clear whether the supplier can pass some of those increased costs on to the customer. As with every other aspect of a supplier relationship, risk will now be part of negotiations.

One effective means for anticipating and planning for discontinuities within extended networks is strategic simulation, also known as war-gaming. (See "Understanding War Games: A Tool for Vulnerability/Discontinuity Assessment," page 21.) Assessing vulnerability is not a new application for strategic simulation, which has been around since the Chinese invented Go 4,000 years ago, but it has taken on

heightened significance since September 11.

Just as security has become a critical consideration in dealing with suppliers, so must it become a factor in evaluating strategic alliances outside the supply chain. For many firms, the reflex reaction to the September 11 attacks will be to pull back from alliances — in particular, global, cross-border partnerships. We believe, however, that alliances may be the safest form of international expansion. Acquiring global assets, which was always risky for operational and cultural reasons, now increases an organization's vulnerability to physical attack as well. A network of alliances, appropriately managed, is potentially more resilient than a collection of global acquisitions. Alliance partners retain local management, eliminating the costs and risks of deploying employees around the globe.

At the same time, a network of alliances represents a substantial interdependence risk for the enterprise, introducing a new set of business perils that are not well understood. These interdependence risks are not technological mysteries so deeply embedded in the mechanics of the Web that you need a computer science degree to understand them. In fact, they are concepts that have been dealt with in various forms for years (for example, PERT charts for program planning). Effectively addressing this risk helps companies deal with important issues such as accessibility to critical information, protection of proprietary information, accountability, and traceability of transactions.

Even before the terrorist attacks, the mounting protests that began in Seattle and continued through Geneva, Davos, and Genoa indicated a need for companies to rethink their globalization strategies. This is not to equate the protesters with the terrorists. But the simple social and economic truth is that there is a palpable opposition in the East and West to the globalization regimens of many multinational companies. French farmers demonstrating against McDonald's as a symbol of American cultural hegemony garnered widespread support despite the company's claim that 80 percent of the products they served were made in France.

At the least, corporate leaders will have to be able to identify legitimate nongovernmental organizations, distinguish genuine grievances from untenable demands, and adapt strategies and operations to the needs of increasingly diverse global constituencies. More important, corporate leaders should add to their companies' mission the goal of spreading the benefits of openness — through education, training, and rising living standards — to the world's dispossessed. In short, the same good corporate citizenship that motivates support for worthy causes at home also should encourage companies to undertake prominent and effective efforts to improve conditions wherever they operate or sell.

When the Chevron Corporation wanted to develop oil and gas reserves in the eastern half of New Guinea, it entered into a partnership with the World Wildlife Fund (WWF) to ensure environmental compliance in an area whose unique ecology is a global treasure. The WWF has offices and monitoring stations at two Chevron camps. "The environment inside the oil fields is actually in much better shape than outside the fields," the physiologist and Pulitzer Prize–winning author Jared Diamond told *strategy+business* last year. "They're probably the best protected national park between the Himalayas and California." Globalization, Professor Diamond concluded, "has enriched New Guinea; it has brought to New Guinea lots of stuff from the outside — computers and management skills and petroleum engineers." Globalization benefited Chevron as well, not only by allowing it to continue to develop a rich resource, but also by providing platforms to develop best practices that are then shared in locations around the world.

Public Policy Formation

Even as they learn new ways to operate on a global stage, CEOs need to be more mindful than ever of the delicate relationship between enterprise and government at home.

Strategic security will require a new, negotiated balance between private companies and the public sector generally — cooperation that doesn't always come naturally. Just as it has become less common in political circles to rail against "big government," so will industry leaders need to recognize that lawmakers are not the enemy. For chief executives, the relegitimization of government means it is time to invest more time and resources in furthering the public–private partnership. This is not the time for adversarial mind-sets, nor is it time to turn to lobbyists to carry the message. Helping legislators craft appropriate security standards will indeed be an integral part of your business strategy.

With power grids, banking networks, industrial logistics systems, and telecommunications networks subject to disruption, mitigating the antagonisms and inefficiencies in the public–private sector relationship will be crucial in preserving citizen trust in the economic system. It will also save lives.

Some things did change forever on September 11. Americans know they are vulnerable now, even in the homeland, the way Britons, Israelis, and Peruvians have known it for many years. America's opponents know that if they can get scale and financing, they can inflict terrible damage, and Americans know that, too.

At the same time, if the war on terrorism is pursued and the coalition holds, our foes will have less and less opportunity. Given the size and spread of the American economy, including what is driven globally by American enterprise, the world has an economic interest in helping America win the war on terrorism. If not, the inevitable

result is more isolationism, and the consequences of that, no matter what it means to America, will be far worse for the rest of the world.

At this moment in history, it is difficult to imagine a scenario that returns us to the picture of unhindered prosperity we imagined not long ago. But imagine yourself a business leader at the outbreak of the U.S. Civil War, not knowing that the United States and Europe were on the verge of the Industrial Revolution. Similarly, there was no way to envision the economic expansion — in the United States as well as in Europe, and later in Asia — that followed the devastation wreaked by World War II.

At each moment in history, business leaders have had to understand the forces that were shaping their world and to work those forces to their advantage — and the wider population's — through profound and fundamental changes. As the forces of terror and freedom continue to battle, the organizations that survive and prosper will be those that recognize the interdependence of openness and security, and that craft strategies to bolster both. ✚

Resources

Randall Rothenberg, "Jared Diamond: The Thought Leader Interview," *s+b*, Third Quarter 2001; www.strategy-business.com/press/article/?art=14916&pg=0

Ralph Shrader and Mike McConnell, "Security, Strategy, and the Commercial Enterprise," *s+b enews*, November 1, 2001; www.strategy-business.com/press/enewsarticle/?art=27934&pg=0

The Constellation Organization: Organizing to Win in the 21st Century, Booz Allen Hamilton Viewpoint, May 2001; www.boozallen.com

"War-gaming: Exploring the Future of Defense," May 2001; www.boozallen.com

Peter F. Drucker, *The Age of Discontinuity: Guidelines to Our Changing Society* (Harper & Row, 1969)

Cyrus Freidheim, *The Trillion-Dollar Enterprise: How the Alliance Revolution Will Transform Global Business* (Perseus Books, 1998)

John R. Harbison and Peter Pekar, Jr., *Smart Alliances: A Practical Guide to Repeatable Success* (Jossey-Bass Inc., 1998)

Network Theory's New Math

Network Theory's New Math

by Michael Schrage

Some are born connected, others achieve connection, still others have connectedness thrust upon them. Everyone is networked. Everyone is either a node or a hub in someone else's network. Much as the quality of life is influenced by the quality of our networks, our standard of living is increasingly determined by network standards. To paraphrase Marshall McLuhan, we shape our networks and then our networks shape us.

The notion of networks as a dominant organizing principle to explain how the world really works has attracted enormous interdisciplinary interest. Physicists are talking to mathematicians who are talking to sociologists and economists who are talking to physicists. In barely a decade, networks of researchers have sprung up to research networks. Executives are beginning to turn to these experts for usable insights into the network dynamics shaping both threats and opportunities in business. (See "Karen Stephenson's Quantum Theory of Trust," page 38, for more on networks and the corporate organization.)

This is no surprise. Transportation networks have striking similarities to telecommunications networks. The Internet's technological behaviors map well onto the ecological behaviors of the biosphere. The complex interconnections between people in research laboratories around the world can be cost-effectively etched onto the design of silicon chips. Similarly, the myriad networks that define corporate connectedness are alike. Economies aren't merely marketplaces; they're networks. Executives need to understand network forces, not just market forces.

As Albert-László Barabási, author of *Linked: The New Science of Networks* (Perseus Publishing, 2002), writes, "The diversity of networks in business and the economy is mind-boggling. There are policy networks, ownership networks, collaboration networks, organizational networks, network marketing — you name it. It would be impossible to integrate these diverse interactions into a single all-encompassing web. Yet no matter what organizational level we look at, the same robust and universal laws that govern nature's webs seem to greet us."

These laws of networks may prove as robust and universal as Newton's laws of motion. But making network laws, which like Newtonian laws are steeped in mathematics and metaphor, comprehensible to the layperson is hard work. The *New Yorker*'s Malcolm Gladwell took a successful first cut with his best-selling *The Tipping Point: How Little Things Can Make a Big Difference* (Little, Brown and Company, 2000). Three new books published this year go far beyond tipping points to present to the conceptually curious reader important theories that reveal the hidden order of complex networks.

Barabási, the author of *Linked*, is a physicist and leading researcher in the field who uses the Internet as his dominant research medium for analyzing the peculiar properties of networks. His book is ideal for those looking for the perspective of a network researcher and practitioner; it's even spiced with a few equations. Mark Buchanan's *Nexus: Small Worlds and the Groundbreaking Science of Networks* (W.W. Norton & Company, 2002) is the product of a physics Ph.D. who writes for the noted scientific journals *Nature* and *New Scientist*. Although Buchanan draws heavily on Barabási's work, his intellectual focus is the intriguing so-called small-world networking theories of mathematicians Duncan Watts and Steve Strogatz. Small-world theories, which are derived from theoretical mathematics and practical reality, prove that seemingly distant, disconnected, and disparate populations, events, or actions can be easily linked to one another. Like many scientists-turned-writers, Buchanan is a bit of an ideologue who seems more comfortable discussing network ecologies than network economics. Then again, because of the transcendent nature of networks, the distinctions between ecology and economics aren't that great.

The least scientific but perhaps most stimulating work for business readers among the three is Howard Rheingold's *Smart Mobs: The Next Social Revolution* (Perseus Publishing, 2002). Rheingold is neither scientist nor technologist, but he knows how to talk with those who are and extract the essence of their thinking and concerns. His previous books on virtual reality, virtual communities, and the history of digital innovation in Silicon Valley remain cult classics for the digerati. What makes *Smart Mobs* so intriguing is not Rheingold's ongoing love affair with the potential of network technology, but his sure grasp of how people play with that potential.

Network Mathematics

Executives interested in the possible impact of network mathematics on their busi-

nesses and industries have a superb analogy from financial innovation, the Nobel Prize–winning Black-Merton-Scholes option-pricing equations. The mathematics was as much a machine tool for creating options as a diagnostic tool for analyzing them. Clever "quants" could use the equations to spot "hidden options" in financial instruments and wring profits from them, or, alternatively, use the equations to customize innovative financial instruments for their clients. Today, an increasing number of firms use real options as mathematical tools for pricing the risks associated with their own business investments.

What Black-Merton-Scholes equations have done for financial innovation and risk, the new network math discussed in *Linked* and *Nexus* will ultimately do for network innovation. Scientists and innovators will look for "hidden networks" within complex systems to figure out whether those networks are being overly relied upon or foolishly underexploited. These analyses will transform how organizations manage their networks to manage value. Indeed, individuals and institutions may be able to create just-in-time network activity to increase reliability and exploit opportunity, much as Black-Merton-Scholes equations empowered innovative traders to create just-in-time trading of options and derivatives to better hedge or speculate. In manufacturing, supply chains represent nothing if not an organizational opportunity to identify hidden networks of risk and reward.

Consider a speculative example from commercial aviation. For decades, American Airlines committed itself to a hub-and-spoke network topology where the vast majority of flights fed into a few key airports. The economics of this network structure worked for a time, but has fallen prey to, among other things, ruthless competition from lower-cost competitors like Southwest Airlines and JetBlue Airways. Southwest dismisses American's hub-and-spoke network approach in favor of its own point-to-point structure. And yet, as Southwest continues to expand and sees flight densities increase at key airports such as San Jose, Oakland, and Las Vegas, isn't it possible that the company will have inadvertently — if not serendipitously — created "virtual hubs" worthy of profitable exploitation. Barabási, Buchanan, and Rheingold would answer with a resounding yes! According to small-world theory, networks emerge from links that were never intended to mesh together. So networks aren't just designed; they evolve.

Order and Randomness

As described in *Nexus*, the ideas underlying Watts and Strogatz's "small worlds" are simple, powerful, and compelling. In effect, Watts and Strogatz validated the "six degrees of separation" phenomenon, the belief that any two people on earth are separated by no more than five people connected to each other in some meaningful way.

Inspired by earlier research on social networks, the two struggled to find a coherent mathematical way to describe how these networks were connected. What Watts and Strogatz found was counterintuitive and profound: By injecting just a few random connections into a complex network, they could make that network both more efficient and more effective. The right random links create small worlds from vast complexities. Randomness can dramatically improve the performance of a complex system rather than ruining it.

When Watts and Strogatz published a paper on their small-world theories in *Nature* in 1998, it "touched off a storm of further work across many fields of science," Buchanan writes. "A version of their small-world geometry appears to lie behind the structure of crucial proteins in our bodies, the food webs of our ecosystems, and even the grammar and structure of the language we use. It is the architectural secret of the Internet and despite its apparent simplicity is in all ways a new geometrical and architectural idea of immense importance."

This finding on randomness has already had a significant impact on the design of telecommunications networks and silicon chips. Microprocessor companies like Intel and Motorola now use elements of small-world theory to link circuits on their semiconductors to make them run faster and more efficiently. Engineers are now aggressively exploring the role of randomness in performance enhancement of their products. Purely rational design that once treated randomness as the enemy has been transformed; designers now play with randomness as a tool to create "small worlds" that exploit this power of serendipitous connection. The result is more robust networks and ever-faster silicon chips. These innovations wouldn't have occurred without the proofs outlined by Watts and Strogatz.

It's important to remember — and this theme is stressed in each of the books — that small-world theory findings are the direct result of interdisciplinary interaction and observation. Empirical observation is just as important as clever theory. The beauty of the small-world hypotheses is that they can be tested in the real world very quickly.

Power Laws

Random geometries of small worlds is just one network law that commands respect. While ambitious managers read Machiavelli to better understand the laws of social and political power, effective executives need to understand that mathematical "power laws" profoundly shape laws of personal power.

"If you are not a physicist or mathematician, most likely you have never heard of power laws," asserts Barabási. In *Linked*, executives will recognize their importance, because power laws can reveal as much about marketing and finance as they

do about math and physics.

The "power" in power laws is not a function of Machiavellian manipulation but the "power" found in exponential functions; numbers squared or cubed or taken to the 10th power, etc. Power laws strike at the heart of what businesspeople think they understand about playing the odds and managing risk. Why? Because power laws are the sworn enemy of a basic statistical concept: the notion that probabilities present themselves in the average distribution of bell-shaped curves. In a networked world ruled by power laws, the bell curve is a dangerous lie.

In fact, power laws describe a radically different kind of distribution. There are no peaks; no symmetries; no bell curve. Power laws look nothing like traditional school-taught statistics. Yet they do a far better job of reflecting how much of the real world behaves. The distinguishing feature of a power law, Barabási writes, is that its distribution is wildly skewed: numerous tiny events coexist within the few very large ones that actually matter.

The distribution of individual wealth in the United States is an excellent example of a power law; a relatively tiny number of people account for the overwhelming majority of individual net worth. The distribution of American and European height, however, is not a power law. There are not a few hundred giants over 1,000 feet tall and millions of pygmies; there's a more comforting and symmetrical bell curve distribution. Power laws explain why computing "the average" — the means, medians, and modes — for insight is so frequently a fool's errand.

Power laws are thus crucial to understand because they force us to look at those few critical hubs — the O'Hares and Heathrows — that dominate either the creation of network value or its destruction. "If Watts and Strogatz's discovery of random connections was a first step into the world of disorderly and complex networks," Buchanan comments, "then the recognition of hubs and power law patterns for the distribution of links is second."

But recall the Southwest Airlines network evolution question: Precisely when does a lowly node evolve into a hub? When should small worlds–oriented sociologists, economists, or mathematicians declare a cluster of nodes a hub? How can we be sure a network's links and hubs are distributed by power laws instead of bell curves? When do a few random connections between networks create more chaos than cost-effectiveness?

The answers to those questions aren't yet known. Networks have laws, all right, but even laws are subject to interpretation and experimentation. The true test of the laws in the context of business and economics will come from the technologies used and abused by Rheingold's "smart mobs."

Reputation Marks the Spot

Smart mobs are a sociological phenomenon that Rheingold persuasively argues will become an everyday reality. These aren't the mobs that storm the Bastille or riot in the streets (although they could); they're small worlds of individuals linked and melded by technological networks, especially through mobile communications. Smart mobs don't just mediate information and analysis; they mediate passion and behavior.

Where *Linked* and *Nexus* describe how networks behave, *Smart Mobs* simply yet expansively describes how people behave — and misbehave — within networks. Rheingold is particularly interested in the just-in-time virtual marketplaces that networks can create on the basis of trust and reputation. "A field known as 'experimental economics' has extended game theory into two specific 'minigames': the 'Ultimatum Game' and the 'Public Goods Game,'" he writes. "Research using these games as probes indicates that:

- People tend to exhibit more generosity than a strategy of self-interest predicts.
- People will penalize cheaters, even at some expense to themselves.
- These tendencies and the emotions that accompany them influence individuals to behave in ways that benefit the group."

In other words, e-Marketplaces are media as much for social interactions as they are for financial transactions. That is, who you are and what you're doing are as important as what you want to buy or what you want to sell. It's no accident that eBay is still around and making money for both itself and its, ahem, community of auctioneers. Your reputation on eBay can — and often does — matter far more than what you are attempting to either buy or sell.

"Reputation marks the spot where technology and cooperation converge," Rheingold writes. "The most long-lasting social effects of technology always go beyond the quantitative efficiency of doing old things more quickly or more cheaply. The most profoundly transformative potential of connecting human social proclivities to the efficiency of information technologies is the chance to do new things together, the potential for cooperating on scales and in ways never before possible."

And yet, when novel "networks of scale," as Rheingold describes them, actually emerge, Barabási and Buchanan insist they will be shaped by the algorithmic imperatives of small-world theory and power laws. People can't break these laws of networks any more than they can violate Newton's laws of motion.

However, mathematical laws can be slavishly obeyed or cleverly exploited. Indeed, as Newton himself once remarked, "To master nature, one must obey her." Scientific laws can empower even where they seem limiting. Entrepreneurs and innovators will figure out how to master networks while obeying their (apparent) laws.

What is Intel without the ideology of Moore's Law? What is the options and derivatives marketplace without Black, Merton, and Scholes? It's still too early to say how the laws of networks will shape tomorrow's technologies and sociologies. But it's not too soon to argue that more individuals and institutions will be more inextricably intertwined with more networks in the future. So you shouldn't read these books with the expectation of rewriting business plans or revising capital expenditures. You should use them to better understand the networks your business has, and to rethink what they should be. Perhaps, in the process, you may discover more than one small world among the disconnected parts of your organization and marketplace. +

Karen Stephenson's Quantum Theory of Trust

Karen Stephenson's Quantum Theory of Trust

by Art Kleiner

Think back to a conversation you had months ago with someone you know well enough to trust, but with whom you haven't spoken since. Chances are you'll remember only vague outlines of the exchange. Call the person and raise the same subject again, though, and more likely than not, the two of you will find yourselves picking up where you left off, remembering the details of significance and expanding into new areas.

To Karen Stephenson, a maverick yet influential social network theorist, the association between trust and learning is an instrument of vast, if frequently untapped, organizational power. The act of reconnecting and talking with a trusted colleague generally triggers a resurgence of mutual memory, opening the gates to fresh learning and invention. This phenomenon, Professor Stephenson contends, is just one example of the direct cognitive connection between the amount of trust in an organization and its members' ability to develop and deploy tacit knowledge together. Because networks of trust release so much cognitive capability, they can (and often do) have far more influence over the fortunes and failures of companies from day to day and year to year than the official hierarchy.

"People have at their very fingertips, at the tips of their brains, tremendous amounts of tacit knowledge, which are not captured in our computer systems or on paper," says Professor Stephenson. "Trust is the utility through which this knowledge flows."

Much has been written about the value of trust. Such social scientists as Francis Fukuyama, Mark Granovetter, and Robert Putnam have made strong cases that high-trust societies have an enormous competitive advantage over legalistic societies, in which suspicion of people is a cultural value, because the transaction costs go down. In high-trust organizations, transaction costs are similarly lower. For example, if people in two different departments or regions (say, marketing and sales, or Asia and Europe) feel enough trust to speak candidly together about their impressions of the market, the quality of work processes, and ways to improve the work, then they have many more opportunities to innovate and think together. The cost of new projects goes down accordingly. Whether high trust applies to a country or a company, the outcome is the same: More value is created when expensive, unwieldy oversight is reduced.

Professor Stephenson's concept, which she calls the "quantum theory of trust," explains not just how to recognize the collective cognitive capability of organizations, but how to cultivate and increase it. At age 50, Professor Stephenson is the most visible member (particularly in business circles) of a small but growing academic field called social network analysis. Originally derived from the complex math used to explain subatomic physics, it is being used to understand and manage the ineffable forces of human interaction within an organization's walls — particularly those forces that can't be captured in formal structures, such as pay scales and reporting relationships, but that implicitly govern the fate of every enterprise.

"The organization chart basically shows you the formal rules. But the ropes of the organization, how it actually works, is the human network," says futurist Thornton May, one of Professor Stephenson's former colleagues at the John E. Anderson Graduate School of Management at the University of California at Los Angeles, where she taught for most of the 1990s. "Karen, more than anyone else, knows how to make it visible."

A trim woman, slight in stature, with large eyes set wide apart and graying hair cut straight and short, Karen Stephenson lectures at a rapid-fire pace, with twangy, slightly tongue-in-cheek forthrightness. She has not written a book to promote her work (preferring to patent her algorithms instead), and you won't find her name on lists of top management gurus. Her academic reputation is one of contrariness; she walked away from a tenured position at UCLA because she didn't like the direction in which the business school was moving.

Professor Stephenson came to management theory after studying the fine arts, anthropology, and chemistry; she talks about organizations as if they were still lifes, researches them as if they were tribes, and plots their decisions as if they were chemical reactions. She is simultaneously a management academic (teaching at Harvard's School of Design and Imperial College's School of Management at the University of London), a computer software entrepreneur (her company, NetForm International, holds the patents on a set of software algorithms for analyzing human networks), and a consultant on the nature of networks in large organizations, particularly as vehicles for change.

She helped J.P. Morgan & Company merge with the Chase Manhattan Corporation, Steelcase Inc. design a new furniture consultation service, IBM reengineer itself, and Hewlett-Packard Company foster innovation. Since the events of September 11, 2001, she has also become a military researcher. Under the auspices of a new government contracting firm, she is helping the U.S. Defense Advanced Research Projects Agency's Information Awareness Office (the counterterrorism branch of the same government research agency that created the original design of the Internet) draw inferences about the weak links in Al Qaeda's network.

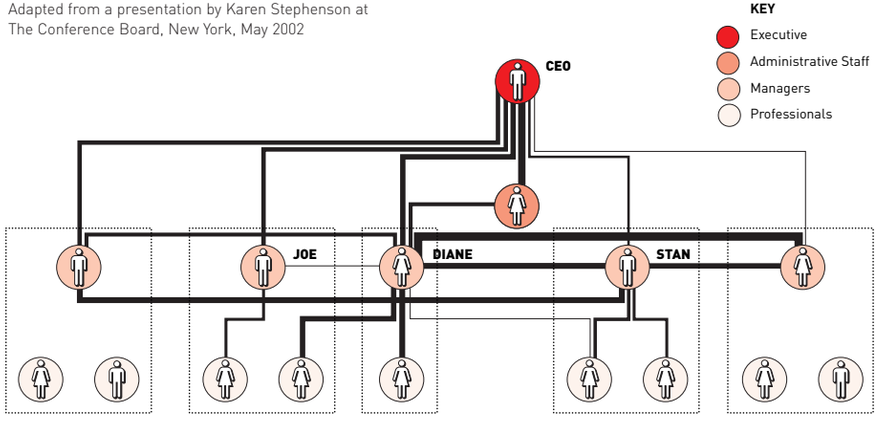
In all these assignments, her research documents what savvy managers have always known intuitively: The form and substance of talk in an organization is as palpably influential on performance as a magnetic field is on a cluster of iron filings. Companies, she says, can exert far greater control over their competitiveness and their future than most researchers have ever thought possible, by putting the right people in the right places and fostering new opportunities for them to talk with each other.

Anatomy of a Network

To understand Professor Stephenson's work, start with the conventional image of an organization: the hierarchy, as represented by any formal organization chart. Then imagine laying over it diagrams of various other kinds showing human networks that are influential within the organization. One overlay might depict day-to-day assignment contacts, which Professor Stephenson calls the "work network." Another diagram might show the social network — people who spend time together outside work. A third might show whom people turn to for career guidance (the career advice network).

Exhibit 1: **Work Network**

Adapted from a presentation by Karen Stephenson at The Conference Board, New York, May 2002



Like the transparencies in a medical textbook, organizational network diagrams all reveal different circulatory systems, but instead of showing the flow of blood, they depict the circulation of information. The data charted in these diagrams could be gathered in various ways (direct observation, tracking e-mails, reading minutes of meetings), but, in practice, network researchers tend to rely on surveys. Karen Stephenson requires at least 80 percent of the people in organizations she analyzes to fill out confidential questionnaires that ask them to name those they work with personally, those they turn to for career advice, those they look to for new ideas or creative collaboration, and those with whom they socialize.

The results can help explain even the most puzzling successes and failures. Consider one case Professor Stephenson researched: the flawed CEO succession in a new R&D subsidiary of a major telecommunications company, which harmed the company's profitability. The story, based on surveys Professor Stephenson conducted, is revealed in Exhibits 1 through 3.

These diagrams show the connections for four key people: the CEO, then nearing retirement, and three of his direct reports, Joe, Diane, and Stan. Those three, like most senior executives, were richly connected to others at the company, but the qualities of their connections were different. Diane, for example, was critical to the day-to-day work of the enterprise. Exhibit 1, the diagram of the work network, shows it: Among the 15 other people included in this chart, seven worked with Diane every day. She was exceptionally plugged in because of her superior knowledge of the company's key technologies.

Professor Stephenson, in fact, refers to Diane as a "hub" in the work network: an individual so well connected to others that she plays an indispensable role in

Exhibit 2: **Social Network**

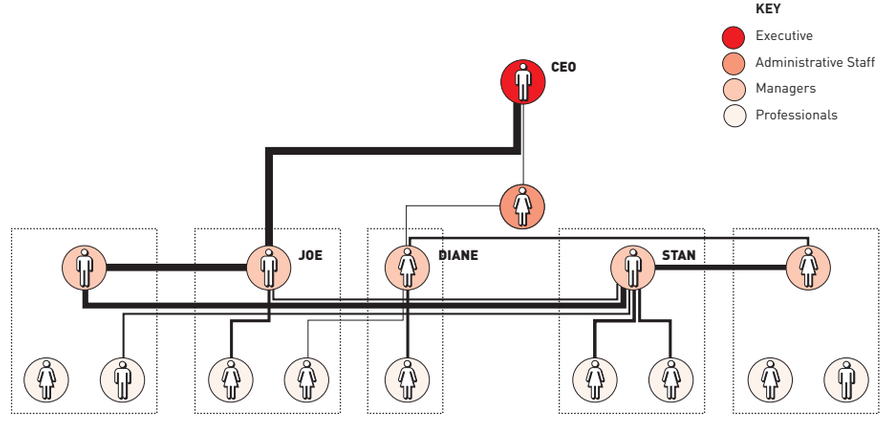
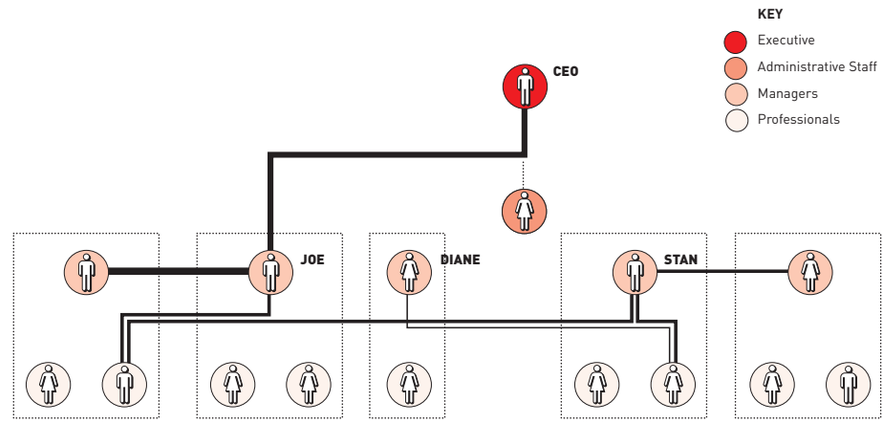


Exhibit 3: **Career Advice Network**



keeping the flow of information going. Hubs are characterized, Professor Stephenson says, by an extraordinarily high level of trust: People know what to expect from them. Their calls are returned. They attend all the key meetings. They convey news. Those who worked closely with Diane, for instance, hardly needed to speak to each other directly; she became their main communication channel.

But Diane's social links (Exhibit 2) and her career advice network (Exhibit 3) are minimal. She was, in short, a workaholic whom everyone depended on but nobody felt close to. "She was sick of her work colleagues," says Professor Stephenson, "and just wanted to go home at night and veg out."

Diane also was a time bomb. She wanted desperately to be promoted to a higher position, believed she deserved it, and felt almost disenchanted enough to leave the company. "Remember, knowledge in this company was generated through mutual trust and exchange," says Professor Stephenson. "If Diane, God forbid, died in a plane crash, a lot of that company's capability would be gone."

Diane's polar opposite was Joe, another of the CEO's direct reports. In Exhibit 1, there is only one thin link between Joe and Diane, representing the minimum collaboration that they absolutely could not avoid. "These two executives actually did not see eye to eye," says Professor Stephenson.

Joe, as it happens, was not very knowledgeable about the company's technology or business, nor did he get much trust or respect from others in the organization. But he had one enormous asset: a strong social bond with the CEO, represented by the thick line in Exhibit 2. Joe and the CEO regularly played golf, and afterward, on the "19th hole," as Professor Stephenson puts it, they plotted the future of the company. For this CEO, socializing outside work with Joe had come to substitute for all other meaningful learning contacts. That, in turn, had weakened the organization and made it far more difficult for him to choose a successor. Because all of this was taking place in a turbulent and highly competitive business environment with an overloaded staff, nobody thought to speak out about the lack of balance in the CEO's network.

Then the CEO retired and passed the mantle to Joe. Diane left the firm. Joe tried to use his connections with others as a surrogate for the knowledge he lacked — and whether intentionally or not, they made it difficult for him to do so. Joe was quickly dismissed by the board, after three months of terrible performance that could have permanently crippled the company. "Someone like Joe, who is neither knowledgeable in himself nor connected within a network of trust, is at high risk of being undermined by others or failing," says Professor Stephenson.

As it happened, however, with Diane and Joe out of the picture, there was now room for a third individual, Stan, to step into the CEO's position. Stan's work connection with the CEO had been fairly weak, and he was only moderately well-connected in the social network. However, Stan was strong in the career network; he met regularly with three other people to make sense of the organization and its future direction and to plot its common course. This was enough to give other people throughout the organization a sense that they could rely on Stan, and that was enough for the board to recognize his value and appoint him CEO. Stan had always kept himself in the background, but he turned out to be very competent. In the next few years, the division recouped much of its performance and profitability, although it never regained the growth momentum that was squandered when Diane left.

The effectiveness and power of an individual, in short, depends not just on his or her position in the hierarchy, but on the person's place in a variety of intertwined networks.

If you were to plug all the data from Professor Stephenson's questionnaires into network modeling software (as she does), you would end up with a series of maps much more complex than the ones shown in Exhibits 1 through 3, showing a large number of possible networks. Professor Stephenson tends to focus on six networks: the three described in this anecdote, plus networks of innovators, established experts, and process improvers. (See the "Six Varieties of Knowledge Networks," page 48.) A typical social network analysis uncovers and tracks the number of links among individuals in any of these networks, the frequency with which people communicate, the relative significance of their communication, and the number of people through which a message passes. Looking at these maps of informal networks, you start to see, as Professor Stephenson puts it, "how the network itself has an intelligence, more than the sum of its parts and beyond the cognition of any one individual."

You also see how to intervene far more effectively. Although the telecommunications company weathered its divisional succession crisis, a preliminary network analysis would have exposed hidden staff problems and opportunities. It would have shown how overburdened Diane was, and it would have helped a savvy leader cultivate her far more effectively — by reorienting her job and setting aside time for her to codify her knowledge or impart it to others. It would have identified Stan as a quiet but highly significant potential leader, so he could have been made part of the management team earlier. It would have made clear the extent to which Joe needed leadership development. It also would have identified up-and-comers lower in the hierarchy. Perhaps most important, an analysis would have given someone (a trusted head of human resources, perhaps) the ability to approach the CEO and say, "There's a lot going on that you are not aware of, and it's affecting your capability and that of the entire division."

Double-Helix Management

Professor Stephenson doesn't suggest replacing hierarchies with networks. Rather, she sees organizations as a sort of double-helix system, with hierarchy and networks perpetually influencing each other, ideally co-evolving over time to become more effective.

But if a CEO wants to strengthen a hierarchy, he or she can also use networks to do so, by establishing new relationships based on three kinds of network "nodes" — categories of people whose personalities and patterns of relationships crop up again and again in the software analyses. The first of these is the hub, the kind of person who becomes a gathering and sharing point for critical information. Hubs show up on network maps like the centers of star clusters, sometimes with dozens of links radiating out from them. Diane, the frustrated subordinate in the CEO succession story, was a key hub because she had what Professor Stephenson calls "centrality": She ranked high as a connector among people; the shortest route to the information needed about work assignments was often through Diane.

Stan, the executive who eventually became CEO, was a different kind of network archetype, a "pulsetaker." Pulsetakers, says Professor Stephenson, carefully cultivate relationships that allow them to monitor the ongoing health and direction of the organization. It's not always easy to tell who the pulsetakers are.

"Even I, after 30 years of research, can't see them by staring at the diagrams," she says. "You can only detect them through the mathematics" — by which she means the algorithmic analysis of survey data. A pulsetaker's patterns of connection show a distinct mathematical pattern, with links that are relatively sparse, but frequently used and diverse. Every now and then someone gets colloquially recognized as the first to sense changes in the wind, and to intervene in subtle but powerful ways. Professor Stephenson likens them to "prairie dogs, poking their heads above the cubicle tops to see what's going on." They make good CEOs in times of crisis, Professor Stephenson says.

The third key type of individual is the "gatekeeper." Gatekeepers are information bottlenecks, controlling the flow of contact to a particular part of the organization, thus making themselves indispensable. In many manufacturing companies, managers of key assembly plants are well known as gatekeepers, protecting the plant's integrity (and their own position) by keeping a tight rein on the information flowing in either direction between the plant and the rest of the company.

Although hubs, pulsetakers, and gatekeepers are Professor Stephenson's terminology, the ideas are not unique. The hub concept is a long-standing artifact of social network research, and gatekeepers were first identified by Massachusetts Institute of Technology professor Thomas J. Allen, Jr. Professor Stephenson, however, has taken the research beyond description and into prescription, suggesting ways to intervene and improve the organization, literally by putting people into different roles based on their capacities as networkers.

"If I wanted to increase learning in a company," she says, "I would take a gatekeeper in an innovation network and put him or her with a pulsetaker in an expert network. That's an algorithm for facilitating the distribution of knowledge."

Professor Stephenson's work has come to seem less counterintuitive in the last year or two, especially as an organization like Al Qaeda has demonstrated how powerful informal connections can be.

Then there is the growing awareness that ideas and trends, like epidemics, spread in nonlinear fashion, with the makeup of human contact being the most important factor. *New Yorker* writer Malcolm Gladwell described this concept in his bestseller *The Tipping Point: How Little Things Can Make a Big Difference* (Little, Brown & Company, 2000). He was later introduced to Professor Stephenson at a dinner party convened by a Saatchi & Saatchi executive — someone who was a "hub" in Professor Stephenson's terms, or a "connector" in Mr. Gladwell's — who knew them both. He immediately recognized her as not just a kindred spirit, but someone who had applied research rigor to the phenomenon that he had popularized.

"My whole thesis is that certain people play critical networking roles," says Mr. Gladwell. "Karen can actually go to a company and point them out. And yet her work is quite subversive in a certain way. It's hard to accept the idea that there are people who play critical roles who don't show up on the organization chart. I've never heard anyone say, 'This person is a powerful networker, and deserves a raise.' But Karen gives us a tool for measuring the contribution of these social types."

Six Varieties of Knowledge Networks

In any culture, says Karen Stephenson, there are at least six core layers of knowledge, each with its own informal network of people exchanging conversation. Everybody moves in all the networks, but different people play different roles in each; a hub in one may be a gatekeeper in another. The questions listed here are not the precise questions used in surveys. These vary on the basis of the needs of each workplace and other research considerations ("Don't try this at home," says Professor Stephenson), but they show the basic building blocks of an organization's cultural makeup.

1. The Work Network. (With whom do you exchange information as part of your daily work routines?) The everyday contacts of routinized operations represent the habitual, mundane "resting pulse" of a culture. "The functions and dysfunctions; the favors and flaws always become evident here," says Professor Stephenson.

2. The Social Network. (With whom do you "check in," inside and outside the office, to find out what is going on?) This is important primarily as an indicator of the trust within a culture. Healthy organizations are those whose numbers fall within a normative range, with enough social "tensile strength" to withstand stress and uncertainty, but not so much that they are overdemanding of people's personal time and invested social capital.

3. The Innovation Network. (With whom do you collaborate or kick around new ideas?) There is a guilelessness and childlike wonderment to conversations conducted in this network, as people talk openly about their perceptions, ideas, and experiments. For instance, "Why do we use four separate assembly lines where three would do?" Or, "Hey, let's try it and see what happens!" Key people in this network take a dim view of tradition and may clash with the keepers of corporate lore and expertise, dismissing them as relics.

4. The Expert Knowledge Network. (To whom do you turn for expertise or advice?) Organizations have core networks whose key members hold the critical and established, yet tacit, knowledge of the enterprise. Like the Coca-Cola formula, this kind of knowledge is frequently kept secret. Key people in this network are often threatened by innovation; they're likely to clash with innovators and think of them as "undisciplined."

5. The Career Guidance or Strategic Network. (Whom do you go to for advice about the future?) If people tend to rely on others in the same company for mentoring and career guidance, then that in itself indicates a high level of trust. This network often directly influences corporate strategy; decisions about careers and strategic moves, after all, are both focused on the future.

6. The Learning Network. (Whom do you work with to improve existing processes or methods?) Key people in this network may end up as bridges between hubs in the expert and innovation networks, translating between the old guard and the new. Since most people are afraid of genuine change, this network tends to lie dormant until the change awakens a renewed sense of trust. "It takes a tough kind of love," says Professor Stephenson, "to entrust people to tell you what they know about your established habits, rules, and practices."

Analyzing Interdependence

Social network theory evolved from studies outside corporations — for instance, of indigenous communities in New Guinea adopting new ideas, or of the spread of HIV through sexual contact. The field is based on the idea that the modeling techniques theoretical physicists use to study subatomic particles can be applied to build elaborate computer simulations of something equally complex: the patterns of contact and colloquy among human beings. (For more on the mathematics behind social network theory, see "Network Theory's New Math," page 29.)

The conclusions that network researchers reach have a way of illuminating the otherwise unexplainable mysteries of organizational triumphs and disasters. Traditional system analysis methods such as econometrics "assume that everybody acts independently," says Carnegie Mellon University professor David Krackhardt, editor of the *Journal of Social Structure*, one of the field's leading scholarly publications. "Network analysis," he adds, "does just the opposite. It assumes that everyone is interdependent. It provides a kind of pattern recognition that makes sense of the complex relationships among people: Here are the bottlenecks; here are the points that are essential to a system, so that if you remove that node, the network falls apart."

Maria Leo, a senior human resources executive at Merrill Lynch & Company during the late 1990s, who commissioned Professor Stephenson for a study of the company's human resources function, calls social network analysis "a high-level MRI of the organization.

"From that, you're able to dig down deeply and use the data to have an effect on people," she says. At Merrill Lynch, she discovered that the most effective recruitment managers were hubs: They stayed in close contact with most of their field personnel, and this led directly to a higher "hit ratio," the proportion of interviews that led to actual hires. She conducted one-on-one counseling sessions with other human resources managers, showing them how more hublike behavior could benefit their departments.

Professor Stephenson also works regularly with a half-dozen architecture and design firms, including the pioneering office furniture manufacturer Steelcase. Partly on the basis of her network theories, Steelcase established a practice called community-based planning. When embarking on an office design for a client, Steelcase conducts a Stephenson-style network analysis of the communication flows, along with a more conventional videocamera analysis of the current workspace ambiance. The designers then reveal the results to the employees who will be working in the new office environment, and invite everyone to design the new setting together. One of the first testing grounds of this approach was an NCR Corporation design facility in

Dundee, Scotland; the employees gathered around giant diagrams of "work networks" and "decision-making networks" projected on wall-sized whiteboards to figure out who would need to be located near whom to promote casual contact.

"There are multiple factors influencing how you might lay out a floor," says Jim Prendergast, a principal with Perkins and Will, an international workplace design firm with which Professor Stephenson works regularly. "They include the geometry of the building, the functions of the hierarchy, the rhythms of door openings, and the axis of circulation. But all of those are essentially abstractions. Karen's work reminds us of the key human relationships that can get stretched, or even destroyed, if the design is based only on these abstractions."

Molecular Studies

The design initiatives, plus a fair amount of business press, have made Professor Stephenson prominent among social network researchers, but she is far from a hub in either management or academic circles. She rarely goes to conferences and doesn't take part in many research colloquies. Although she teaches at three schools (Harvard, the University of London, and the Stevens Institute of Technology in Hoboken, New Jersey), her primary office is a three-room suite in a warren of creative studios above the Strand bookstore in Greenwich Village, New York.

Professor Stephenson's interest in social networks dates to her undergraduate years majoring in art and chemistry at Austin College in Texas, where she discovered that she had a predilection for pattern recognition. In art history classes, she could recognize not just the artist of a work, but the date, by reading the characteristics of the brush strokes. She began selling her own paintings to New York galleries, then grew disillusioned with art and moved to the University of Utah to study quantum chemistry.

But instead of submolecular particles, she became interested in people. While managing the 200-person chemistry lab, she began to notice that the kinds of radioactive degradation she saw in macromolecular chemistry were not that different from the patterns of communication breakdowns and rivalry that she saw in the lab. "There was more to calculus than devising formulas for describing the shape of space," she says. "There was also a calculus of human exchange." This led her to an interest in the archaeological record of ancient trading patterns, the oldest available data about the roots of human exchange. And that, in turn, led her to a shift of academic field, to anthropology; she began to conduct field archaeology research in the Middle East. A paper she wrote about algorithms for analyzing trade networks caught the eye of Carl Lamberg-Karlovsky, director of the Peabody Museum, who introduced her to Harvard's anthropology department, which accepted her as a Ph.D. candidate. Working part-time in labs and then technology businesses to support her studies, she began to see today's organizations as modern-day equivalents to the trade networks of ancient times.

In her doctoral dissertation on the technology company Bolt, Beranek and Newman (BBN), Professor Stephenson (with Harvard statistical scientist Marvin Zelen) devised a formula for ranking the significance of individuals as knowledge conduits. Information scientists at BBN, which was founded by MIT professors as an acoustic-design company, had invented (among other things) the packet-switching technology underlying the Internet and had chosen the @ symbol for use in e-mail addresses. Interestingly, researchers at the Harvard Business School had been trying, unsuccessfully, to get permission to conduct a case study on this highly innovative company for 25 years. Ms. Stephenson, however, was the first prospective researcher from the school of anthropology. It turned out that BBN cofounder Richard Bolt, who was still active in the firm, had been close friends with Margaret Mead. In Ms. Stephenson's interview with him, he said, "Well, if anyone can understand us, an anthropologist should." She began to use the formula from her dissertation to calculate how networks changed over time, working initially at Harvard, then as a UCLA faculty member, and currently from her offices in New York.

Trust and Transactions

For all of Professor Stephenson's observations about the value of trust, there's a cloak-and-dagger quality to her demeanor, particularly when she is figuring out whether to take on an assignment. She seems to alternate between open enthusiasm and suspicion; it's as if her own theories have sensitized her to the flip side of trust: betrayal. But once she is fully committed, she digs deep into the heart of the organization, conducting analyses over the course of a year or two. Because she must interview or survey so many people to do an analysis, she claims to have the largest data bank of business network survey results in the world.

Often, Professor Stephenson enters a company through the human resources department to research what is seen as a personnel problem. She came to Merrill Lynch to help explore why some human resources managers were more effective than others. But inevitably, she touches on strategic issues, because the organization's ability to implement any new strategy depends primarily on the way knowledge courses through its networks. If the CEO is a hub, that makes a difference; if a gatekeeper dominates a particular strategic product or region, that makes another kind of difference. And if the relationships between top executives and others are devoid of trust, or if key sources of information in the informal networks are not formally recognized or rewarded, that can paralyze an organization.

"All along, I've been implicitly studying trust," says Professor Stephenson. "But I only came to a full realization of it in the last couple of years."

Professor Stephenson's quantum theory of trust holds great potential as a diagnostic method for the unquantifiable aspects of business. Imagine that at any given moment, you could analyze the health of an organization's networks. For instance, a company might have a healthy work network (with a great deal of open information flow about processes and very little workaholism), a medium-grade social network (with little real contact but also little pressure), and a low-quality network for what Professor Stephenson calls "continuous improvement" — the ability to innovate new processes easily. Any organization can be stunted in one of these areas and bountiful in another.

Professor Stephenson suggests that most organizations do not remain static. Their network health profiles continually change. An organization's path from one network health profile to another not only is predictable, she says, it can be influenced. There are archetypal patterns that repeat, over and over, and, depending on the prevalent pattern, make it possible for one company to thrive where another fails. A startup technology company might begin with a low work/high social/medium improvement profile, as people first get to know each other. Then, as venture capital and deadlines kick in, the profile would move to high social/high work/medium improvement. And then there might be a betrayal by one of the senior executives. At this moment, the fate of the company's networks hangs in the balance. Does its improvement capability, for instance, go up or down? Does its social capability flatten to the point where people leave the company? Or can the strength of the networks, fortified by the trust people feel for one another, override the crisis?

Part of Professor Stephenson's current research is devoted to tracking the patterns of movement from one network profile to another, patterns that recur from organization to organization. "It's like a Rubik's cube," she says, "turning in three dimensions, with the organization spiraling through the various quadrants in a helix-like motion over time." She is also articulating the factors that make the most difference in moving the networks in healthier directions — factors in which trust is always central. For example, one easy way to improve the level of trust, anytime and anywhere, is simply to increase the speed with which people respond to communication. When people return our calls or e-mails quickly, it sends a signal that we can rely on them because our connection, however distant, is important enough to claim some of their attention. "Human beings always keep an internal accounting system of who owes what to whom," says Steve Haeckel, director of strategic studies at IBM's Advanced Business Institute, who has collaborated with Professor Stephenson for 10 years on some of the trust-related research she's done. "Response time is one indicator of the degree of trustworthiness of the other individual."

You can also weaken trust in networks by removing key people. This approach to altering networks takes on particular relevance in Professor Stephenson's current work with the Defense Department's research agency. She is working with the agency to identify key nodes of Al Qaeda and other terrorist networks; undermining trust within those networks may be as effective a form of defense against them as, say, attacking their remaining strongholds with military force.

It may seem unnerving to think of networks as something that can be undermined or manipulated; after all, they are composed of human friendship and behavior. But politicians and leaders (as well as novelists and dramatists) have long known, if only intuitively, how a mere word of betrayal or trust, or the movement of a particular key person from one spot to another, can significantly change an outcome. Professor Stephenson's theories, if they turn out to be correct, will simply provide a scientific underpinning for this awareness — and a far more powerful and reliable capability, for those who choose to use it.

And there lies the rub for the rest of us. Do we want to live in a world where people, even those with the best of intentions, have this kind of power to disrupt and reshape networks? Or perhaps we already live in such a world, and it's up to us to engender the kind of trust that will, in the end, make it palatable to remain there. +

Resources

Joel Garreau, "Disconnect the Dots," *Washington Post*, September 16, 2001

Malcolm Gladwell, "Designs for Working," *The New Yorker*, December 11, 2000; www.netform.com/html/newyorker.pdf

Albert-László Barabási, *Linked: The New Science of Networks* (Perseus Publishing, 2002)

Howard Rheingold, *Smart Mobs: The Next Social Revolution* (Perseus Publishing, 2002)

Journal of Social Structure: www2.heinz.cmu.edu/project/INSNA/joss/index1.html

NetForm International: www.netform.com

Responding to Systemic Shocks

Enterprise Resilience: Managing Risk in the Networked Economy
By Randy Starr, Jim Newfrock, and Michael Delurey
First published in *strategy+business*, Spring 2003

Beyond Utopia: The Realist's Guide to Supply Chain Management
By Keith Oliver, Anne Chung, and Nick Samanich
First published in *strategy+business*, Second Quarter 2001

Supply Chain Surprises
By Ed Frey, Steve Nied, and Barry Jaruzelski
First published in *strategy+business* as "Balance-Sheet Fix: No Orphaned Orders," First Quarter 2002

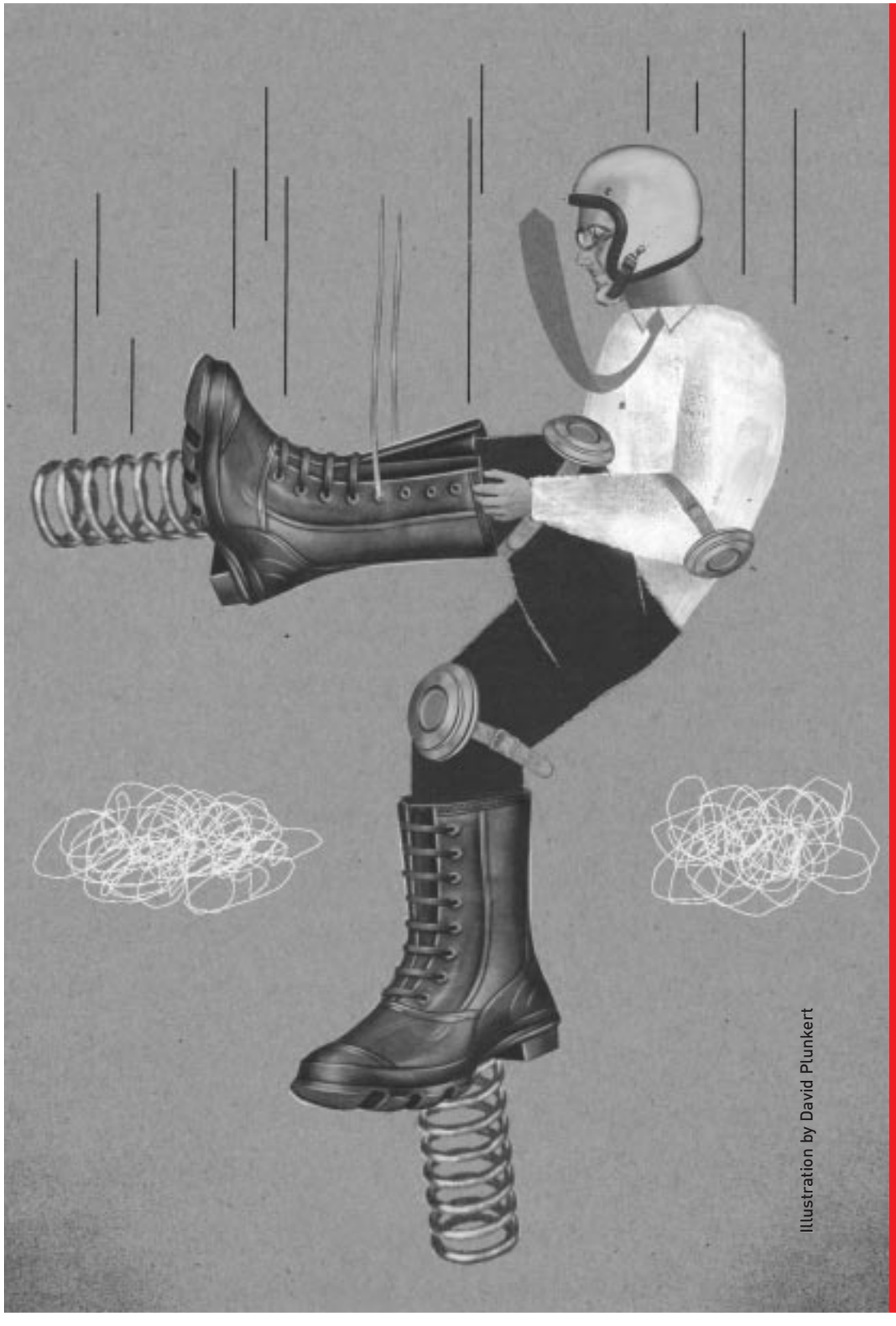


Illustration by David Plunkert

Enterprise Resilience: Managing Risk in the Networked Economy

Enterprise Resilience: Managing Risk in the Networked Economy

by Randy Starr, Jim Newfrock, and Michael Delurey

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

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

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

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

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

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

The Adaptation Imperative

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

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

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

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

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

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

Interdependence Risk

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

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

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

Diagnose Your Enterprise Resilience: Eight Fundamental Questions

- Are the complexity of the extended enterprise and major earnings drivers across it transparent?
- Are interdependencies understood and interdependence risks identified?
- What programs are in place to ensure the viability of earnings drivers?
- Are these programs fully aligned with corporate strategy and objectives, and do we understand the trade-offs within these programs?
- Do we know what we spend on resilience?
- How good is our situational awareness — that is, do we have enough business intelligence, internal and external, and is it directed to the appropriate parties?
- Do we distill such intelligence properly and in a timely enough fashion to react to it?
- Who is accountable for resilience, and how do we make decisions and measure progress?

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

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

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

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

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

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

War-Gaming and Resilience Planning

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

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

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

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

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

— R.S., J.N., and M.D.

ER vs. ERM

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

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

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

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

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

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

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

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

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

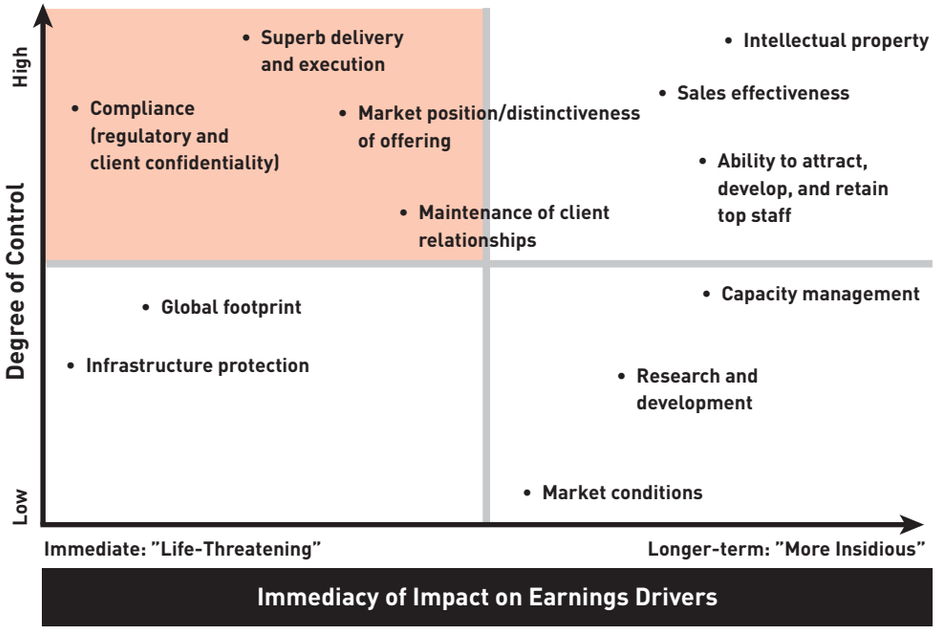
There are three essential steps to becoming a resilient enterprise:

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

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

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

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



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

The ER Audit

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

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

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

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

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

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

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

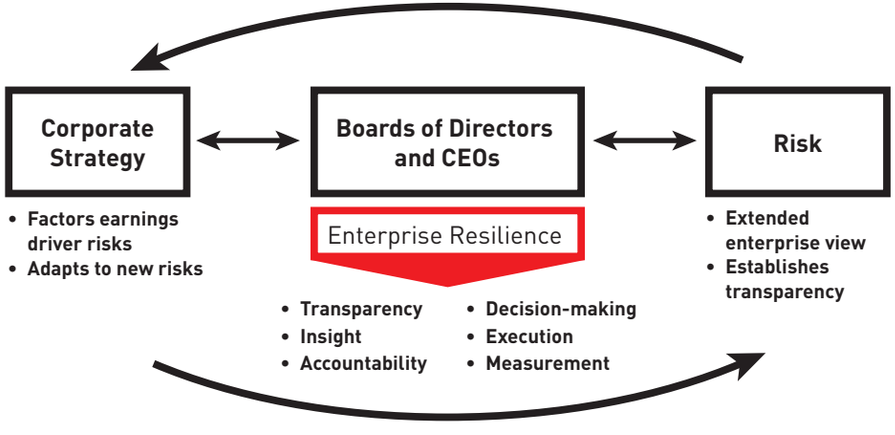
By contrast, even the largest advertising agency could get by without too much damage if it lost its computers for a day or longer. However, an ad agency must pro-

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

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

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

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



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

Risk Is Reality

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

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

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

Resources

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

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

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

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

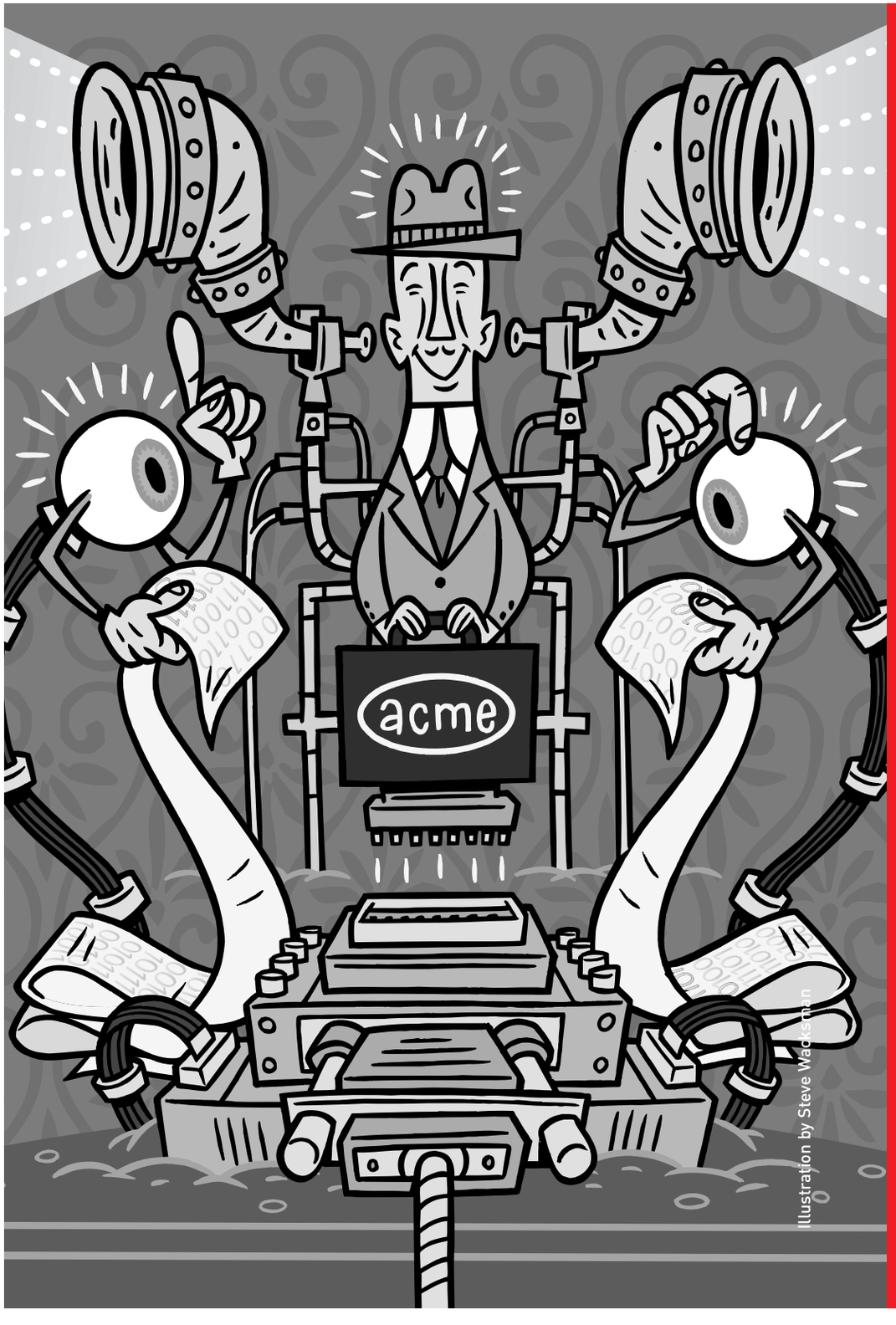


Illustration by Steve Wackerman

Beyond Utopia: The Realist's Guide to Supply Chain Management

Beyond Utopia: The Realist's Guide to Supply Chain Management

by Keith Oliver, Anne Chung, and Nick Samanich

For decades, academics, economic philosophers, and Communist dictators dreamed of a Utopia founded upon a planned economy. In this magical place, an elite intelligentsia with perfect data, analyses, and insight would plan and control economic life; in this place the distortions of the market would be eliminated.

The central planning concept clearly failed in its most radical form, the economies of the former Eastern Bloc. Yet today, core elements of the central planner's Utopian dream live on in academic papers, in the business press, and in the sales brochures of uncounted software and technology vendors. Nowhere is this fantasy more evident than in supply chain management. Armed with more real-time data, a better algorithm, more connectivity, and a bigger IT budget, managers (or their computers), the dreamers believe, could control their extended enterprise free of market imperfection.

The Internet seems to be on the verge of turning such wishes into reality. Wireless technologies make it easier than ever to monitor inventories and equipment remotely and to track orders and trucks in real time. Web-enabled tools allow companies to view operational details of the partners in their supply network and to track demand at point-of-sale. Emerging tools are beginning to offer promises of seamlessly linked supply chains that — fueled by real-time data — will coordinate and ultimately optimize supply chain networks across the extended enterprise. The term extended enterprise resource planning (eERP) has begun to appear in the press to describe this phenomenon.

We believe that attempts to create the Utopian planned supply chain will ultimately fail. Although we have no doubt there is true value to be gleaned from emerging capabilities, we also believe there is risk in becoming too enamored of their potential. We hold a more sober (but, in our opinion, more realistic) view of how companies can leverage emerging technologies to move toward the goal of achieving more effective supply chains. The key lies not in gaining more visibility or computational power, but in enabling supply chain partners to align business objectives and reengineer the supply chain across the extended enterprise. We call this approach Federated Planning.

Supply Chain Management: The Evolution

Supply chain management has changed little since Booz Allen Hamilton introduced the term in 1982. Historically, functions — from procurement through manufacturing, distribution, sales, and marketing — "owned" parts of the supply chain. Conflicting objectives and distortions between and among them led to delays, excess capacity, and excess inventory throughout the supply chain. Booz Allen's supply chain management approach called for an overarching supply chain strategy and control architecture to align functional activities with business objectives. (See Exhibit 1.)

Strategy determined how assets were deployed to meet service and cost objectives, driving manufacturing footprint, inventory, and production allocation decisions. Policies, rules, and procedures, which together make up what we call control architecture, managed assets to meet customers' needs. This control architecture defined replenishment, planning, and scheduling processes and policies, and supported metrics, systems, and organizations. A control framework defined the hierarchy of supply chain management and processes that aligned functional activities at each level.

Exhibit 1: **Supply Chain Management Hierarchy**

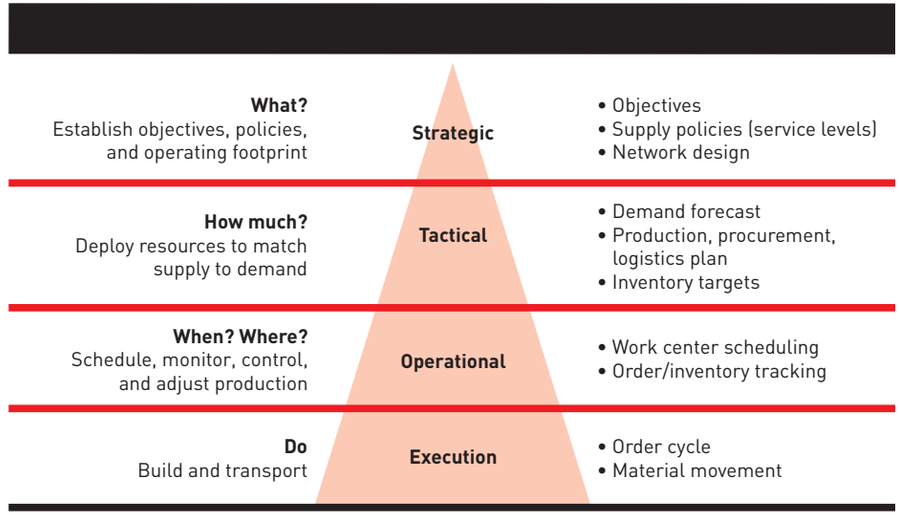
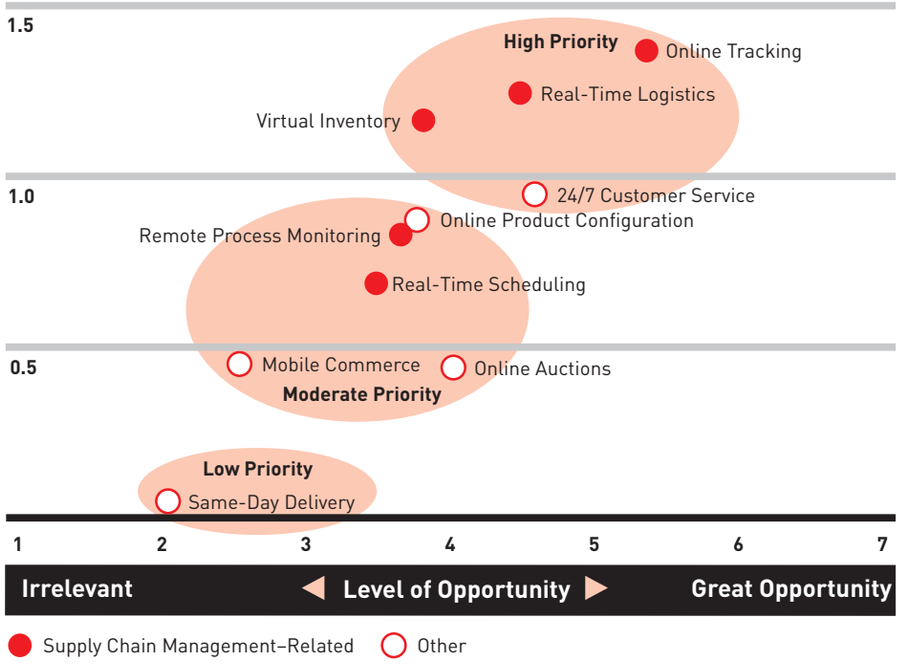


Exhibit 2: **Executive Survey of Prominent Technology-Enabled Service**



Over the years, supply chain management efforts seemingly were hampered by gaps in information: inaccurate demand statements, lack of visibility into current order and supply positions, and incomplete understanding of costs, capabilities, and constraints. Companies were forced to hold excess capacity and inventory as they second-guessed demand projections, delivery schedules, and capacity and material availability across the supply chain.

The Internet has promised to change all that. Web-enabled tools offer complete visibility and communication across the extended enterprise, delivering perfect information with the potential to eliminate waste throughout the supply chain. With that promise, supply chain management is moving to the forefront of business strategy in many industries — and capturing the attention of senior management. In a July 2000 survey conducted by Booz Allen Hamilton, Fortune 500 senior executives ranked tools such as real-time logistics planning, remote process monitoring, and online order tracking high in opportunity, but thought their companies did not have the capabilities in place to take advantage of them soon. (See Exhibit 2.)

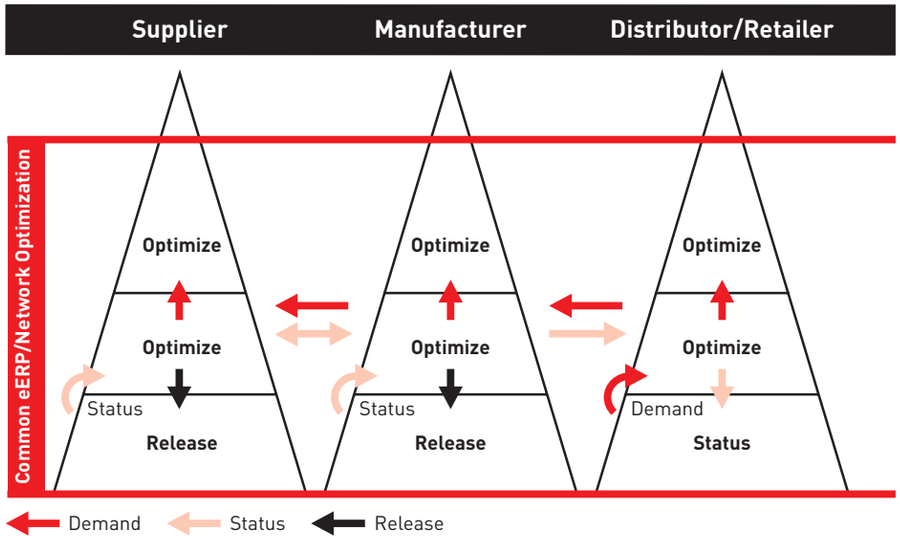
This renewed interest in supply chain management is well founded. Expanding market reach, greater customer focus, and increasing market and cost pressures are forcing many companies to reevaluate the effectiveness of their supply chains. The increasing compression of concept-to-launch cycles and product life cycles is mandating more flexibility and agility in supply chains than they have ever had before. As many industries undergo difficult transitions, they are focusing more sharply on supply chain partners to improve supply chain capabilities and economics. Collaborative planning, or the cooperation by supply chain partners to achieve more accurate forecasts and plans, is now widely touted as the next revolution in supply chain management.

Not surprisingly, the consumer products industry has been at the forefront of the collaborative planning movement. However, even after a decade of such initiatives as Efficient Consumer Response and Direct Store Delivery, the consumer products industry still carries, on average, 14 weeks of inventory, which represents $300 billion in goods trapped in the supply chain. Clearly, improved collaboration among supply chain partners is needed to further increase efficiency and reduce inventory.

In 1994, a coalition of consumer products manufacturers, retailers, software vendors, and IT consultants launched the Collaborative Planning, Forecasting, and Replenishment (CPFR) initiative to create a standard protocol for exchanging data between supply chain partners. Several pilot efforts have shown notable success among companies exchanging plan and forecast data. In one example, Nabisco Inc. and Wegmans Food Markets Inc., a U.S. grocery chain, improved category sales for Planters nuts by 13 percent — compared with an 8 percent drop in the market — and reduced inventory by 18 percent while improving the service level from 93 percent to 97 percent. Although such pilots demonstrate the benefit of sharing plan and forecast data, how CPFR will manage the complexity, and conflicting objectives and priorities, of multiple supply partners is unclear. As Jay Nearnberg of Warner-Lambert Company (now part of Pfizer), one of the pioneering CPFR companies, states, "CPFR seems to work with a single manufacturer collaborating with a single retailer. Whether it will have the same results when multiple manufacturers collaborate with the retailer for the same product [has] yet to be tested."

Collaborative planning is looking to move beyond the periodic sharing of plan and forecast data through Web-enabled visibility tools. These tools will allow companies to share detailed data across the extended enterprise, accessing point-of-sale data at the stock keeping unit (SKU) level and status of orders and shipments in real time. Early successes promise huge potential. For example, Ford Motor Company and UPS Logistics, a wholly owned subsidiary of United Parcel Service Inc., launched an effort to reduce the time it takes vehicles to reach dealers from assembly plants — historically, two weeks. Through vehicle-level tracking that improved coordination among rail cars, trucks, and haul-away tractors, UPS has already

Exhibit 3: **Extended Enterprise Resource Planning Approach**



reduced transit time for new Ford, Lincoln, and Mercury brands by four days since March 2000, saving $1 billion in vehicle inventory and more than $125 million in inventory-carrying cost.

Bring on the Vendors

With a promise so great, it seems only natural that visibility and collaboration tools should be linked, allowing management and optimization of the supply chain through the use of real-time data. A host of vendors are developing systems to collect such detailed, real-time data at each tier in the supply chain and to coordinate the flow of goods across the extended enterprise. Some are developing massive optimization algorithms that will evaluate and redefine supply structure in response to real-time data. Some envision systems that will seamlessly link supply chain partners through a common system, a conduit for all information flow and controls throughout the supply chain — a concept some are referring to as an eERP system. The system would synchronize activities across the supply chain to trigger machines and trucks into motion; reset production mix and volume; reallocate resources; and, when linked to Advanced Planning, Scheduling, and Network Optimization tools, optimize the integrated supply network. (See Exhibit 3.)

Proponents of eERP suggest that with a common understanding of the supply universe, participants would work toward a common goal of maximizing profit for the whole. Priorities and conflicts would be resolved objectively by an eERP system that worked to achieve optimum solutions across the extended enterprise. Participants would willingly share sales and production data to maintain the validity of the eERP system. Or, better yet, the system would be directly linked to data sources to ensure that real-time data flowed seamlessly across organizations.

The eERP movement seems to be well under way. Software vendor SAP AG is strengthening its supply chain management capabilities, having added Logistics Execution Systems in 1999, followed by Advanced Planning and Optimizer (APO), a tactical forecasting and network optimization tool. SAP is currently building collaborative planning capabilities into APO, and is positioning itself as a provider of integrated supply chain management solutions. Similarly, the Oracle Corporation recently added a logistics management module to its suite of tools that already included supply chain management. Companies such as i2 Technologies Inc. and Manugistics Group Inc. are becoming full-suite supply chain solution providers; B2B exchanges are positioning supply chain management as a core value offering; and niche technology vendors are scrambling to build relationships with established enterprise resource planning (ERP) and software companies and IT consultants.

The vendors' rush to join the supply chain management bandwagon is understandable. Supply chain management software is projected to grow 47 percent over the next five years; at the same time, ERP growth rate will slow to an anemic 5 percent. Not only will supply chain management tools replicate the heady growth enjoyed by ERP in the late 1990s, but they also promise to employ the armies of IT programmers and consultants displaced by the slowed growth of ERP.

Despite the risk that eERP could bring with it the same ballooning cost and lock-in problems associated with ERP before the "e," executives will find the lure of efficient supply chains difficult to resist. But when software companies come knocking to offer an extended ERP system — promising millions in savings and the mother of all supply chain management tools — companies should proceed with caution.

The idea that independent companies can be joined into a single entity with perfect real-time data and analysis brings us back to our analogy of the Utopian central planner. While the idea of a harmonious, unified supply network is comforting, we believe that this view is overly idealistic and that it severely underestimates tensions and complexities inherent in the supply network. Further, we believe the quest to build a highly responsive, efficient supply chain will create dependence on real-time data that will introduce unnecessary variability and instability into the supply chain, which could ultimately undermine participants' strategic objectives.

First, the Utopian view fails to recognize the tension and conflict in the supply chain that result from competition for limited resources and distribution of profit and risk. In one telling example, the $45 billion U.S. apparel textile industry

launched an effort in 1993 to develop an industry-wide collaborative decision support tool. Industry leaders hoped that understanding the impact of decisions would promote collaboration among the supply web partners, despite decades of competition and mistrust. After six years of work by industry specialists, the Department of Energy, and academics, the goals were not achieved; the project was recently handed off to CPFR. In our opinion, continuing down this path will quickly debilitate the collaborative planning efforts. This example helps prompt our more cynical view that, as conventionally envisioned, collaborative planning efforts will degenerate, with each company working to achieve its own objectives and motivated to withhold valuable information that could be applied to gain an advantageous position in the market, just as they have always done.

Furthermore, the Utopian, single-entity approach severely underestimates the enormity and complexity of the supply chain. In the apparel textile example, 30 synthetic fiber plants, 6,000 textile plants, 20,000 cut-and-sew plants, and 100,000 retail outlets make up a supply chain that conducts more than 20 billion consumer transactions each year. The industry's supply chain is further influenced by the supply chain partnerships for other products within it, each competing for shared resources over the extended supply chain. The textile apparel supply chain, in short, is less a chain than a complex web of intersecting supply chains. Even from the perspective of one company, tens of thousands of nodes make up this supply web, with each node participating in up to hundreds of thousands of production activities each day. Layers of interconnected decisions make it impossible to get a comprehensive view of the supply web. And without understanding a participant's entire set of customers, product lines, economics, capabilities, current practices, and culture, it is difficult to distinguish real supply constraints from those that are imposed by other decisions and assumptions.

Finally, emphasis on real-time data to manage the supply chain introduces unnecessary instability and may inadvertently lead companies away from their strategic intent. Powerful Internet-enabled technologies track point-of-purchase demand at the SKU or outlet level in real time or near–real time, with the possibility of a supply chain that can respond to orders as small as a single unit. However, driving the supply chain at the single-unit demand level introduces unnecessary variability, particularly in industries with unpredictable demand patterns. Without adequate restraints, the optimization model may react to data points, rather than trends, and create wide fluctuations in production planning.

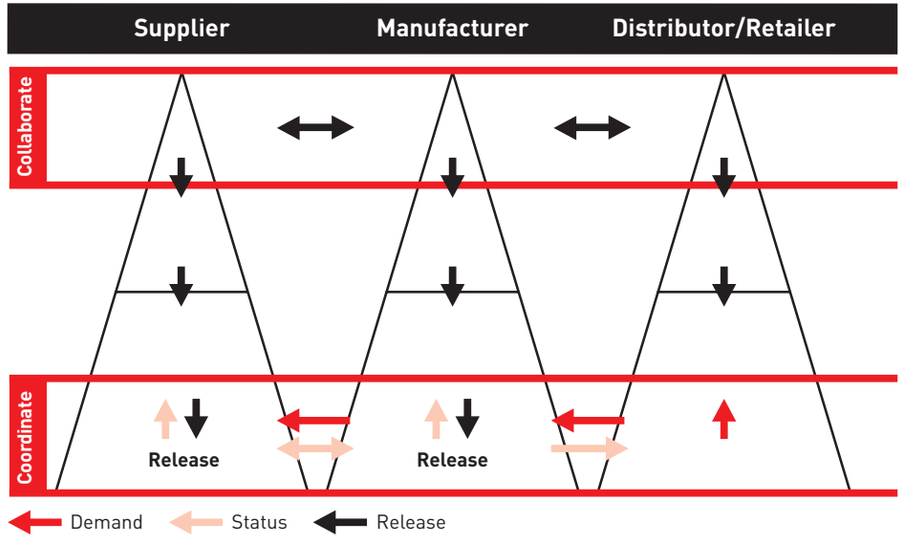
Similarly, eERP systems may respond inappropriately to real-time capacity and supply positions, creating an availability-driven model in which production mix and volume are set to maximize utilization of available resources. Availability-driven models may be appropriate in very simple supply chains or in industries in which supply conditions significantly influence outcomes. For example, in tuna processing, the constraint of fixed facilities and moving supply supports an availability-driven model. However, in most industries, the availability-driven model represents the ultimate "push" production system — and the path to responding to the latest information may inadvertently lead companies away from meeting their overarching supply chain objectives.

Enter Federated Planning

For all these reasons, we believe that the Utopian view of centrally planned extended enterprise management is flawed, and that attempts to optimize the supply chain from the bottom up will ultimately fail. To extend the political analogy, we endorse a federalist view, which recognizes each supply chain partner as an independent entity working to maximize its own objectives and trade-offs as a "citizen" of multiple supply networks.

The Federated Planning approach — based on the federalist view of collaboration among independent entities — is a strategic collaboration process that begins with the alignment of business objectives. Through an iterative process of objectives-driven discussions around cost and service trade-offs, supply chain partners can understand critical constraints and cost drivers in the supply network and achieve agreement on performance levels, incentives, rules, and boundaries. These boundaries define supply policies and targets and govern the flow of information across

Exhibit 4: **Federated Planning Approach**



organizations, allowing supply networks to monitor shifts in the marketplace and to evolve with changing market conditions. (See Exhibit 4.)

Federated Planning is fundamentally different from the Utopian approach in three ways. First, Federated Planning does not attempt to dictate supply chain "solutions" for the extended enterprise, but relies on negotiations among supply network partners to define and manage the supply network. Second, collaboration is achieved through alignment of business objectives, not through the exchange of detailed data. Finally, the federated approach does not attempt to generate a one-time solution, but instead is an iterative process that is designed to shift with changing market conditions. The approach provides the means to explicitly define and manage relationships between supply network partners — based on rules and policies, not transactions — and to monitor trends and trigger a revisiting of supply network decisions.

A hypothetical example illustrates the Federated Planning approach. A consumer-products manufacturer presents to a key supplier a "wish list" of service levels, such as order-to-delivery lead time, fill rate and product selection, and desired pricing. The customer also shares projected demand by mix and potential ranges or uncertainty in demand.

The supplier considers the requirements of this and other customers to determine how best to allocate its resources. Since resources are typically limited, the supplier must make trade-offs between potential customers and products. By understanding implications of cost drivers such as service levels, demand fluctuation, and product variation, the supplier creates a cost-to-serve profile for each customer and product category. The supplier can then define acceptable service levels and pricing to achieve its own business objectives and make preliminary allocations of capacity and other resources by product and customer that optimize its operations.

The supplier reviews its plan with this and other customers. If joint objectives are met, no additional iterations may be necessary. However, in most cases, conflicting objectives will ensure that one or both parties do not meet their business objectives. Or they may believe that there is more "money on the table." In these cases, the supply network partners will work together to achieve a better solution by identifying ways to challenge key constraints and cost drivers. For example, if lead time is a key issue, partners may explore alternative points in the network where inventory can be held, or redefine the components that are produced to forecasted demand versus real demand. These discussions may lead to changes in product configuration that can "desensitize" early stages of the supply network to product mix variations. Or the negotiations may lead to moving final assembly or order aggregation out to customers, or to logistics service providers. To combat capacity constraints, the supplier may consider shifting capacity from another customer or product line, adding another shift, or outsourcing some of its production.

Once alternatives are identified, the manufacturer and supplier retreat to assess the implications independently. Each evaluates service level and cost-to-serve implications by customer segment or product line; their effect on other customers, suppliers, or product lines; and the potential impact on sales, share, branding, or overall ability to achieve short- and long-term business objectives. The manufacturer and the supplier also identify what incentives or trade-offs are needed to achieve agreement. With a more robust understanding of internal cost drivers and constraints, supply partners may identify new alternatives to meet the network cost and service level objectives. The supply partners then return to the joint effort to review the impact of these "what if" scenarios and engage in an iterative process to identify opportunities to break constraints, understand implications, and reach an agreement.

The agreement is defined by a joint commitment to service or performance levels, pricing, and other incentives, and potentially volume or resource allocations. A federated supply network agreement also defines the rules of managing the supply partner relationship. Boundaries or rules are defined that set the conditions under which the supply agreement is valid, and that trigger changes in the network or require the agreement to be revisited. For example, if demand volumes or variability in a market exceed original assumptions, changes in capacity or inventory targets may be required, and pricing or service levels may need to be renegotiated. Similarly, changes in market or supply conditions, such as shifts in raw-material pricing or industry capacity, may trigger new discussions. Rules may also be established at the executional level on how individual orders are triggered, tracked, and coordinated across the network. The agreement also defines the content, format, and frequency of data exchange needed to monitor and maintain this relationship. Similarly, the agreement identifies process or systems requirements.

Becoming Federated

Federated Planning has several advantages over the Utopian approach. It enables supply chain partners to break constraints in the current supply chain, driving step-function improvements. In contrast, traditional network optimization efforts strive to optimize within existing constraints. Most industries have already undertaken numerous efforts to extract supply chain efficiencies, and any additional gains will be difficult to achieve without a paradigm shift.

The federated approach also minimizes complexity. The process of understanding cost drivers, trade-offs, and demand characteristics leads to a natural segmentation of customers and products by service levels and cost-to-serve and to segregation

of products and processes that create "noise" in the system from those with more stable characteristics. Stable products and processes can be managed using simple physical or visual cues, eliminating the need for sophisticated forecasting, planning, or tracking tools. On the remaining products and processes, supply partners can address the source of variability by changing product configuration or assembly processes to move variability as far down the supply chain as possible.

Under Federated Planning, the supply chain continues to evolve to greater efficiency over time. Supply partners naturally align for the most efficient pairing of requirements and capabilities. For example, products with highly unpredictable demand, such as many entertainment, apparel, or consumer technology products, will be aligned with suppliers that can rapidly free up incremental capacity or maintain excess capacity at the lowest cost. That leaves other suppliers to focus on achieving high levels of efficiency on products with more stable demands. And when market conditions, capabilities, and economics change, federated supply networks continue to evolve as supply partnerships realign and supply policies reset to meet demand.

The federated approach requires a far simpler set of technology tools and systems than its Utopian counterpart. The decentralized model calls for a software architecture that supports a layered supply chain management approach, using best-in-class software to support activities within each layer of architecture. The need for massive transaction processing systems and complex tactical planning systems is significantly reduced, as is the need to align business processes and use a common data structure and nomenclature.

Federated Planning requires support tools that build insight into how the supply chain reacts under possible conditions, not tools that attempt to optimize at the detail level. Traditional linear program-based tools like Manugistics, while effective at optimizing product flow within existing supply chains, are incapable of defining or evaluating what does not exist or might be possible. Another approach — stochastic modeling — allows companies to rapidly assess "what-if" scenarios. Stochastic modeling does not involve optimization or simulation, but allows supply chains to be modeled and evaluated rapidly using a hypothesis-driven approach to identify key constraints and cost drivers. Until recently, few stochastic modeling tools were available, leaving companies to pursue in-house development. However, new tools like Greyhound Technologies' Supply Chain Explorer now offer off-the-shelf solutions.

Similarly, the use of appropriate "e-supply chain tools" at all levels of the supply chain will be critical to meeting strategic objectives. Actual or stated capabilities of emerging Internet-enabled supply chain tools will tempt companies to replace management judgment with decision support tools, creating overreliance on tools — and on data to feed the analysis. Companies will need to understand each tool's capabilities, limitations, and optimal application. In most cases, application focused on addressing specific business issues will be far more effective than trying to build an integrated solution to link these capabilities together.

Those who succumb to the Utopian dream of a centrally planned supply chain will soon find themselves mired in the complexities and conflict of the real world. While the federated approach offers neither the valor nor the romance of Utopia, history again will prove that self-interest will ultimately prevail. +

Resources

Scott Buckhout, Edward Frey, and Joseph Nemec Jr., "Making ERP Succeed: Turning Fear into Promise," *s+b*, Second Quarter 1999; www.strategy-business.com/press/article/?art=14866&pg=0

Lawrence M. Fisher, "From Vertical to Virtual: How Nortel's Supplier Alliances Extend the Enterprise," *s+b*, First Quarter 2001; www.strategy-business.com/press/article/?art=17892&pg=0

Timothy M. Laseter, C.V. Ramachandran, and Keith H. Voigt, "Setting Supplier Cost Targets: Getting Beyond the Basics," *s+b*, First Quarter 1997; www.strategy-business.com/press/article/?art=14326&pg=0

Timothy M. Laseter, "Balanced Sourcing: The Honda Way," *s+b*, Fourth Quarter 1998; www.strategy-business.com/press/article/?art=14796&pg=0

Michael Schrage, "Here Comes Hyperinnovation," *s+b*, First Quarter 2001; www.strategy-business.com/press/article/?art=21036&pg=0

Supply Chain Surprises

Supply Chain Surprises

by Ed Frey, Steve Nied, and Barry Jaruzelski

The boom-and-bust cycle of the recent past filled high-tech manufacturers' supply chains with excess materials, prompting them to collectively write off billions in inventory and hundreds of millions in purchase commitments. Yet a potentially greater problem still lurks in the form of off-balance-sheet inventory: goods ordered but no longer needed in the face of the global slowdown. Suppliers possess contracts, orders, and even materials requested by the manufacturers but no longer needed. Traditional inventory metrics capture only goods on the balance sheet. As a result, excess off-balance-sheet commitments and materials — billions of dollars of supplier commitments — often are invisible to management and shareholders. The problem demands attention, as strapped suppliers and contract manufacturers want buyers to make good on their promises.

It is, therefore, critical to manage potential off-balance-sheet liabilities early and proactively. Recent events have shown that failure to disclose off-balance-sheet liabilities can be disastrous. Furthermore, once a supplier makes an actual claim, a manufacturer's options are extremely limited, and the likelihood of a cash payout is quite high, so getting in front of them is critical.

Purchasing organizations traditionally attempt to resolve such claims. But these efforts often are inadequate because they fail to take advantage of corporate leverage and potential "tradeables." Supply chain organizations don't always pay enough attention to looming unfulfilled forecasts and orders until they become real claims. Managing commitments earlier and proactively can help to reduce cash impacts.

Booz Allen Hamilton has identified a five-step process that makes off-balance-sheet inventories visible and allows manufacturers to deal with potential liabilities in an effective manner. Although this approach is designed for the proactive management of potential liabilities, it can also be used to develop a balance-sheet entry for supplier commitments. The steps are:

- Use a company-wide "radar screen" to make off-balance-sheet inventory visible; segment each item by risk of cash impact.
- Manage exposure, with different strategies for each type of potential liability.
- Negotiate at the corporate level with vendors to aggregate all potential liabilities.
- Leverage tradeables to defer cash outlay.
- Establish processes to monitor potential off-balance-sheet liabilities and to respond to problems as they arise.

To deal with off-balance-sheet inventory liabilities, companies must understand their magnitude and risk. Inventory liabilities that could require cash outlay range from "hard" to "soft." "Harder" liabilities pose higher risk, are more difficult to negotiate, and generally have a shorter term than "softer" liabilities. In brief, harder liabilities cost more; softer liabilities can be negotiated down and possibly away.

Potential liabilities tend to move from soft to hard. If obsolescence and forecast reductions are not dealt with in a timely fashion, they can turn into claims. Still, it doesn't make sense to go out and settle every potential liability claim.

The trick is to understand the threat and deal with it appropriately. Many potential liabilities will not turn into hard claims or may take a long time to do so. In those cases, it may be worth taking some risk to keep the cash. In some cases, the supplier doesn't even realize that a liability exists.

Knowing and acting upon the aggregate liabilities from a supplier is critical. Otherwise, you are at risk of getting picked apart by the supplier through many claims spread over time and across your facilities. Although minimizing the payout is one objective of resolving potential liabilities, it should not be the overriding one. Gauge the balance between the health of your balance sheet and the health of the supplier and incorporate it into the negotiation. Look for "win–wins" that will preserve a positive relationship.

In high-tech manufacturing, conserving cash is a high priority. Heavy debt loads, stingy capital markets, and reluctant customers have made cash king. Paying out cash to settle contingent liabilities, even for a fraction of the original promise, could threaten your existence. Since your suppliers want you to continue to be a customer, they may be willing to entertain compensation other than cash.

Managing off-balance-sheet inventory liabilities should not be a one-time event. The tech bust created excess inventory as demand fell off faster and farther than ever experienced previously. However, more than ever before, the tech world has to pay close attention to managing supply chains to optimize inventory levels. Supply chain management is more critical in technology manufacturing for several reasons:

• The popularity of high-tech products and specific configurations has become increasingly unpredictable. Bigger bets are required to capture the upside.
• Outsourcing manufacturing to contract manufacturers and consignment programs shifts on-balance-sheet inventory to off-balance-sheet inventory.
• Traditional buyer–supplier agreements can create conflicting objectives and incentives that result in financial liabilities between layers in the value chain.

The best way to avoid off-balance-sheet inventory liability is to prevent it. Focus supply chain and product management processes on running lean rather than on scaling up. The recent past rewarded manufacturers with supply chains that could scale up and phase in new products quickly. The near future will reward those who run lean supply chains that are as flexible scaling down as up. +

Strategy & Leadership After 9/11

The New Balance Between Risk and Control
By Ralph W. Shrader
First published in *strategy+business*, Fourth Quarter 2000

From New Economy to Siege Economy: Globalization, Foreign Policy, and the CEO Agenda
By Jeffrey E. Garten
First published in *strategy+business*, First Quarter 2002

The Fortune at the Bottom of the Pyramid
By C.K. Prahalad and Stuart L. Hart
First published in *strategy+business*, First Quarter 2002

The New Balance Between Risk and Control

The New Balance Between Risk and Control

by Ralph W. Shrader

Decision-making today places a premium on speed to a degree unprecedented in world history. The need to act in e-time is testing the limits of the command-and-control model that has dominated commercial and military leadership for generations. To maintain a bias for action — and stay centered on the appropriate goals — both realms are coalescing around an emerging leadership model that rebalances traditional attitudes toward two crucial decision factors: risk and control.

In the corporate world today, decision-makers need to have a higher tolerance for and comfort level with risk. Multimonth task forces are the buggy whips of leadership. Today, failure to decide and act quickly can preempt options altogether. Increasingly, companies across industries are managing risk at a portfolio level — something financial services companies have been doing for decades. If one product line or venture doesn't pan out, it's okay, as long as the sum of business decisions yields success.

For the military decision-maker who deals not just in capital assets but in lives and national credibility, the concept of risk has greater implications. Bet-the-company decisions, such as those being made every day now in the Internet industry, would be totally inappropriate on the battlefield. Yet the redefinition of risk in the face of e-time is occurring in this sphere as well.

General Colin L. Powell has warned that procrastination in the hope of reducing risk actually increases risk. He recommends a 40/70 formula, and advises, "Don't take action if you have only enough information to give you less than a 40 percent chance of being right. But don't wait until you have enough facts to be 100 percent sure, because by then, it is almost always too late. Once the information is in the 40 to 70 range, go with your gut."

Contemporary leaders need to heed this advice, and become comfortable making decisions with imperfect data. At the same time, they must create a fault-tolerant culture for those below them in the organization, so the men and women closer to the action can take appropriate risks and make courageous decisions with less fear of failure.

That means contemporary leaders must also be willing to have less personal control — which is the second key element affecting decision-making today.

Leaders have to become more comfortable not knowing it all. This does not mean they have to lose control over situations, or give up responsibility for decisions. But they need to give up control of doing it "our way" in terms of process, and focus instead on setting the vision and driving the desired outcome through participative leadership.

Here again, there is concurrence between what is happening in corporate and military decision-making. As Booz Allen Hamilton war-gaming specialist Mark Herman puts it, "The commander has to maintain 'top sight' — to set the vision and watch that the mission is being met, but not focus on the tactical details about which fighter is going after which target. There isn't time for vertical command and control. There isn't time to direct operations at that level of detail. And the fact is, pilots and navigators are usually in a better position to make those decisions."

Corporate decision-makers need to rely on soldiers in their organization in a similar way. Max DePree, former CEO of Herman Miller Inc., explains it this way in his book, *Leadership Is an Art* (Doubleday Books, 1989): "Participative management guarantees that decisions will not be arbitrary, will not be secret, or closed to questioning. But participative management is not 'democratic.' Having a say differs from having a vote." The best leaders empower and listen to their people — but they take full responsibility for making decisions and for the consequences of those decisions. +

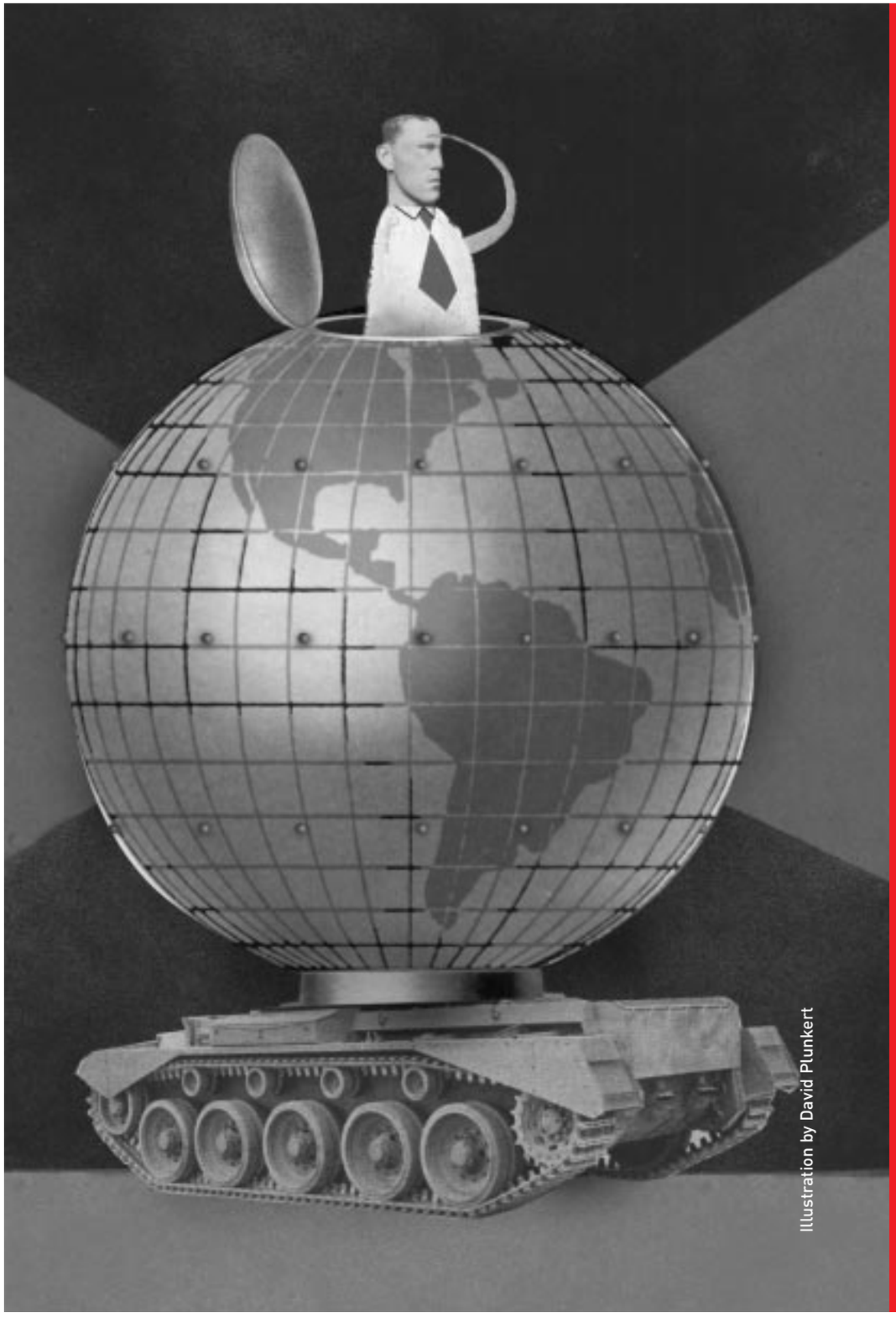


Illustration by David Plunkert

From New Economy to Siege Economy: Globalization, Foreign Policy, and the CEO Agenda

From New Economy to Siege Economy: Globalization, Foreign Policy, and the CEO Agenda

by Jeffrey E. Garten

We tend to think of United States foreign policy as the result of a formal process — the product of diplomatic rounds, bilateral discussions, and official negotiations. But a substantial part of U.S. foreign policy always rests on the overall milieu in Washington at the time.

In the 1990s, that environment was heavily weighted toward commercial interests. There was the push for the North American Free Trade Agreement, the establishment of the World Trade Organization, a blizzard of other trade agreements, an emphasis on strengthening relationships with emerging markets, and a vigorous effort to prevent financial crises from spreading beyond local economies. Most of Washington's economic assistance to other nations was designed to bring about liberalizing economic reform. In short, the U.S. had created a global, outward-looking foreign policy environment.

This liberating spirit became synonymous with the term globalization, and U.S. multinational companies were partners with Washington in promoting this variant of globalization. Corporate leaders sided with the administrations of George Bush (the senior) and Bill Clinton. Backed by a majority of the U.S. Congress, they fought together to level the playing field for global business, waging successful campaigns for greater liberalization of trade and finance, more deregulation, and increased privatization of state-owned enterprises.

Now, the fight against terrorism will dominate American foreign relations for the rest of the Bush administration, and probably beyond. It will influence everything from domestic civil liberties to economic policy to our choices for allies abroad. This new focus represents a sharp discontinuity from the outlook of the last decade. Washington will likely back a different kind of globalization — one focused less on the opportunities for expanded commerce than on addressing the many holes and vulnerabilities in an open economic system. Instead of knocking down barriers, our new war, of necessity, will place more controls on banking, movement of people, and technology exports. The emphasis will be not on reducing the control of government, but on enhancing it in a wide variety of ways. "Homeland security" says it all — domestic-oriented, restricted, more closed than at any time since World War II. In place of an ethos of liberation will be a philosophy of control. In place of a spirit of opportunity will be a feeling of vulnerability. Not long ago we talked about a New Economy. Now we are looking at the possibility of a Siege Economy.

The geopolitics of antiterrorism will substantially alter the prospects and paths of American corporations. For most chief executives of American companies, the new crisis presents issues never before faced: a halt to the headlong, liberating globalization of the past two decades; more regulation of company activities, at home and abroad; and the reintroduction of military and other noncommercial considerations into American foreign policy.

Chief executives of American multinationals would seem to be perfectly placed to team with Washington and the other governments of the free world in reinventing globalization to address the challenges ahead. Within their own organizations, they have had to address many of the social, economic, and geopolitical issues that we used to relegate to government. Their companies have been increasingly reliant on diverse, global work forces. Their profits depend less on extracting raw materials than on mining and sharing knowledge among educated populations of workers and consumers. Understanding the limits of command-and-control management in decentralized organizations, corporate leaders would appear well positioned to become the kind of "business diplomats" the world now needs, as it seeks to develop coalitions to fight a war that takes place on a myriad of physical and virtual fronts.

Unfortunately, CEOs of American multinationals have shown themselves unwilling and unable to shoulder these new responsibilities. In interviewing some 40 chief executives for my book, *The Mind of the CEO*, I discovered that while most of them wanted to play a more statesmanlike role, they felt they had neither the time nor the mandate to do so to any great extent. They felt under too much pressure to meet quarterly earnings targets to do much besides focus on their knitting. Now, however, they have no choice. September 11 — and ensuing events — are rebalancing the relationship between the public and private sectors, forcing a negotiation of interests unlike any seen since World War II. Having spent the last decade and more attempting to make the world safe for globalization, multinational CEOs must now participate in a broad, ongoing effort to make globalization safe for the world.

The Changing Context

Once the initial burst of patriotic fervor subsides, there is a risk that the direction of U.S. foreign policy and the interests of American multinationals will diverge. At a minimum, much more tension will exist between the two than existed before. During the last few decades, American companies have internationalized more than is generally acknowledged. Their production, supply systems, sources of finance, work forces, and management are increasingly global. Many Fortune 500 companies now derive more than 50 percent of their revenues from abroad; for most of the rest, global diversification remains an important objective. The Bush administration, though, is riveted, quite reasonably, on national interests. U.S. CEOs will naturally try to align themselves with the administration. But they will not be able to completely match actions with rhetoric, given their need to balance interests in the U.S. with those outside its borders. The fact is, companies have much more interest in an open world economy than in one focused on increasing regulation.

The trend away from economic openness and liberalization will manifest itself in numerous ways. Among the initial contextual changes CEOs can expect is the increasing politicization of international economic policy. The U.S. will pressure the International Monetary Fund (IMF) and the World Bank to pump funds into countries whose antiterrorism goals are compatible with American goals. The World Trade Organization (WTO) is likely to admit new members, such as Russia, more quickly, even if they have not met the policy prerequisites that China and other nations have had to achieve.

It is a certainty, as well, that Uncle Sam will promise economic inducements to nations that cooperate in the fight against terrorism — incentives that may not have strong linkages to sound economic policies. The large-scale aid packages promised recently to Pakistan and Uzbekistan — countries that were in disrepute with Washington just several months ago — are harbingers of what's to come. The U.S. is also bound to provide trade preferences for countries in the coalition (again, absent the policy reforms that in past years were a quid pro quo for most-favored-nation status), just as it has done recently for Columbia and other Latin American nations as a reward for fighting drug lords.

Other differences between the interests of multinational businesses and those of the government are likely to surface. There is a danger that, in its campaign against terrorism, Washington may not be able to sustain adequate attention to macroeconomic problems that affect the world economy, to the detriment of U.S. firms that have gambled so much on a strong and open international economy. As we enter a global recession, for example, a number of emerging-market economies in Latin America and Asia are in trouble, including Argentina, Brazil, and South Korea. Because they are not on the front lines of the war against terrorism, these countries may not receive the attention they need. Yet if history is a guide, the failure of one or more could become contagious, especially against the backdrop of a rapidly weakening global economy. Short-term debt relief and intervention in the capital markets will go only so far in propping up these faltering economies; long-term direct investment in emerging markets is slowing down, too, indicating that the perils they pose to global economic stability will exist for a long time.

These are not the only global economic challenges brewing. The exchange rate system is more precarious than it has been in a long time; the dollar is overvalued, the yen is being held down by major Japanese intervention that cannot last, and the euro is still to be tested. Japanese banks are in increasingly bad shape, putting more pressure on the global banking system.

Trade tensions loom, too. Japan is looking for a depreciating yen, but the U.S. and other countries are not able to take a flood of imports from Tokyo. China's entry into the WTO isn't the end of the China trade problem. There will be many challenges to China's policies within the WTO, and China will also play a powerful political role in championing the causes that developing countries have pushed, not very effectively, for several years.

America's ability to lead the global economy out of such quagmires may well be compromised by the war on terrorism. The G8, readily persuaded during the 1990s toward liberalization by the strength of the U.S.'s hyper-strong New Economy, could well begin to dismiss any new efforts as disingenuous attempts by Uncle Sam to offset the costs of America's campaign against terror. It's one thing to share intelligence information; it's another to change budgetary and monetary policies.

Costs for Companies

These and other changes in the global economic environment will affect American firms directly and indirectly. Companies will get less support from U.S. government economic agencies, whose activities will be distorted by the fight against terrorism. The Treasury and Commerce departments, which led the successful battles for commercial diplomacy and trade liberalization, will begin to focus more on monitoring and surveillance of finance and trade with terrorist networks. The Export-Import Bank and the Overseas Private Investment Corporation will be preoccupied with helping frontline states in the antiterrorism campaign, largely by gearing their lending and guaranty programs to companies integral to U.S. foreign policy priorities, not global trade and investment in general. It is hard to believe that these and other agencies will have the time and energy to pursue normal commercial goals.

The probable remilitarization of U.S. foreign policy may also prompt a political

backlash against the United States, which could undercut corporate activities abroad. The situation may be similar to that faced by American firms overseas during the height of the Cold War, when many embassies were the object of political attack, and military-to-military links counted more than commercial connections. The stationing of military forces in Central Asia, the increasing interaction between the Pentagon and its counterparts in various countries, and the need to build up clandestine intelligence capabilities all point in this direction. If we align ourselves with repressive regimes abroad to achieve our ends, we would be opening the U.S. and, by extension, its companies to hostility of significant proportions.

We should not underestimate the problems all of this can cause for American firms. Even before September's terrorist attacks, in many quarters "globalization" was synonymous with "Americanization." To many, this had a positive meaning; both terms connoted openness, opportunity, and a market orientation. But to others, "Americanization" implied a harsh form of capitalism, one dismissive of local needs, environments, and traditions. With the U.S. pursuing a high-profile military policy around the world, identification with "Americanization" is unlikely to help U.S. firms, except in those nations that also find the very fabric of life threatened by actual terrorist assault.

At the least, American companies will bear real costs. High on the list will be the cost of security. U.S. companies are prime targets for terrorism overseas — and it shouldn't be forgotten that Wall Street and the very idea of world trade were specific targets of September's attacks. Firms will need to increase protection of their physical facilities (including the building of redundant capabilities), their communications infrastructure, and their people. They will need to vastly enhance security checks of all employees. American executives will have to take more care in traveling. All this is expensive, and will cause U.S. companies to stand out in ways that can only impair their competitiveness. (See "Security and Strategy in the Age of Discontinuity," page 12.)

Competitiveness against corporate rivals from other nations with less foreign policy baggage could be further hindered if the U.S. imposes economic sanctions on other governments based on the needs of its antiterrorism campaign. American companies could, for example, be prevented from operating in certain markets, or they might find trade in certain goods and services curtailed. Conversely, companies might be pressured by Washington to help with the economic dimension of building up weak states that breed terrorism — an activity that companies have shied away from, since they see few commercial benefits.

Crisis-Bred Opportunities

Lest the commercial consequences of the war on terrorism seem unduly dire, remember that crises can be catalysts for positive changes. Chief among them are the opportunities corporate America and Washington now have to build a stronger global system. These opportunities arise from a number of sources.

In contrast to the way he started his administration, President Bush has now made foreign policy a priority. Indeed, he seems to have matured greatly — and remarkably quickly — in the substance and style of being a president. As part of this transformation, the administration has been forced to reverse its knee-jerk antipathy toward multilateral cooperation. It seems to be taking the United Nations more seriously. It understands that it must moderate its earlier peremptory treatment of major countries like Russia, Pakistan, and Iran, and deal as well with weak or failed states, such as Afghanistan and Uzbekistan. All are countries whose cooperation the administration will need for a long time.

The new engagement could be a chance to integrate some of these countries, particularly Russia, further into the world economy. More optimistically, if George W. Bush's antiterrorist campaign evolves in a manner that is seen abroad to be calibrated, proportionate, and effective — that is, if it really succeeds in rooting out terrorists without creating enormous political fallout — then he and his administration will be in a very strong position to lead the world in other, nonmilitary endeavors.

Put another way, there is a chance that the depth of military and political collaboration potentially in the making can be translated into stronger international economic cooperation. As of October, the multicountry coalition being forged was still shallow and precarious, with the notable exception of the U.K.'s participation. But to increase the odds that broad and permanent benefits will come out of the efforts to build an antiterrorist confederation, we need to identify and work toward an end game that both meets and transcends the goal of physical security.

Business and government should collaborate on ways to reenergize global trade negotiations, taking advantage of the new spirit of cooperation between the U.S. and the European Union, the two largest and most powerful trading areas, which can make or break the talks. It was heartening to see the beginning of world trade talks in mid-November 2001. But starting them was the relatively easy part. Making them succeed is another matter.

Surely, this is a time for a trade round that is aimed foremost at integrating developing countries into the global system. These negotiations must be mounted quickly, have a simple agenda, and work on a tight timetable. Now is the time for concrete progress that will boost the world economy, not a five-year marathon.

Even if steps toward extending the benefits of an open global economy into the

developing world prove hard to accomplish, American multinationals are so enmeshed in the global marketplace that they have a great stake in working to prevent a rollback of the economic liberalization that has been achieved in the last 10 years. Perhaps the current crisis can be a wake-up call for those who grew complacent during these last several years of prosperity, thinking they need do little more than ride the waves of globalization.

On the one hand, American multinationals have to push harder for liberalization of trade, finance, and immigration, even as the political headwinds grow stronger. If they don't do this — if they do not champion globalization — no one else will.

But on the other hand, multinationals will have to work with governments to achieve the best balance between openness and security. Business and the public sector can collaborate, for example, on harmonizing important rules of global commerce, such as antitrust regulations or intellectual property rights. Improving the condition of communities in which they operate ought to be an integral feature of businesses' strategy, not out of altruism, but out of self-interest in promoting an environment that at least lessens the chance of becoming a political target.

For government and business, there is a very compelling case for collaborative action. Without underestimating the life-and-death importance of successfully combating terrorism, we should not forget that economic development and progress — and the economic ties among nations that reinforce them — are at the heart of what most societies care about. A long war against terrorism that ignores or undermines that will be counterproductive and probably unsustainable. If economic conditions do not improve for most of the people of the world, the kind of global capitalism that has allowed industrial nations to prosper will cease to exist.

We are closer to that breaking point than we have been in a long time, given the diversion of efforts toward rooting out terrorism around the world.

A Cooperation Agenda

Government–business collaboration can take many forms, from the grand to the particular. There are, for example, some technical fixes that can help keep the global commercial system from unnecessarily grinding down. CEOs and government officials ought to join forces to streamline enhanced customs inspections, to impose as few obstacles as possible in the global commercial logistical system. They can do this with certain embedded technology that allows government officials to inspect cargo long before it crosses borders.

Executives and officials also should cooperate on security issues relating to the nation's information infrastructure, an area where national security, commercial interests, and such social concerns as privacy all overlap. The entire policy of homeland security, dependent as it is on taking into account the workings of the national economy that we so frequently take for granted — the system of transportation, communications, the public health infrastructure, etc. — also needs to be a collaborative effort between the public and private sectors.

CEOs and top government officials should put their heads together to develop a strategy for economic development that isn't simply a series of short-term political payoffs, but builds a solid foundation for market economies to take advantage of the global system. There is a lot to do to strengthen international institutions like the IMF, WTO, and World Bank, as well as to develop new rules for cyberspace and stronger systems for public health — to take the most obvious examples.

Two immediate measures can be enormously helpful. First, because foreign investment in developing countries will fall as companies and institutional investors shy away from all kinds of risk, we need to develop more mechanisms to provide political risk insurance — something that used to exist but was being whittled away as the world seemed to be getting safer and as the role of governments was diminishing in finance. Second, there ought to be an acceleration of efforts to strengthen corporate governance of all kinds — from implementing sounder accounting to protecting investors. In an atmosphere of risk, such mechanisms enhance investment flows, and every little bit will help now.

Washington needs to be prepared to make considerable new investments in multilateral institutions, a departure from the more aloof stance the administration evinced during much of its first year. American businesses ought to be not just highly supportive of but involved in this effort; for example, providing ideas about how they and the World Bank can work more closely together to get effective investment into developing countries.

Both business and government should rethink their political approach to globalization, aiming to add a more humane element to it, with more emphasis on environmental cooperation, education and training of non-U.S. work forces, and the creation of social safety nets in less-developed countries. These policies — descendants of the Marshall Plan programs we supported in Europe after the close of World War II — will not by themselves eliminate terrorism. But the harsher capitalism that has been spreading around the world is not compatible with the need for political support for globalization. At the heart of everything is the need to build a system of commerce that makes as many people as possible feel they have a chance for a better life within the system that is evolving.

Let me try this another way: Some three weeks after the September 11 attacks, the *Financial Times* editorialized that "the ills of the world's poor resulted from too

little globalization, not too much." This is not completely right. Globalization is not an end in itself; sustainable globalization is. CEOs and developed-world officials alike would be remiss were they not to acknowledge that certain effects of globalization have clobbered emerging markets time and again in the last several years. Even before mid-September, increasing attention around the world was paid to the downside of an integrated world economy. There is no question that globalization has widened the gap between rich nations and poor nations, and between rich and poor within countries. The troubles of today — and tomorrow — will be concentrated in those segments of the world that are falling further and further behind. It was tragic enough from a social and moral perspective to live in a world of these widening disparities. But now it holds a tangible security dimension, as well.

So more attention must be given to the impoverished, and a better way of helping them move up the economic ladder, than has been to date. Antiglobalization demonstrators highlighted the problem; because many of them were avowed anarchists or freelance troublemakers, it was easy to dismiss their concerns. But the fact is, many Third World governments were becoming increasingly troubled, too, even before September 11. Their concerns cannot be addressed by either government officials or corporate leaders acting in isolation. (By the way, it wouldn't hurt for CEOs and government leaders to have even the semblance of a strategy to deal with those protest groups, who are getting more and more attention. Surely now is the time to develop one.)

American CEOs further have a role to play in pressing Washington not to neglect policies that were strengthening globalization before September 11, and that are still crucial for the future. A major case in point is our relations with Mexico, much of which were turning on more cooperative ties regarding people flows. It is hard to envision political support in Washington for more liberal immigration policies today. But sooner, rather than later, we will need to have them, even in the context of stepped-up vigilance. We may need to take some detours, to be sure, but we have to get back on the right road.

We must continue the effort to shore up the global banking system, well beyond the new push against money laundering. Similarly, we can't forget the need to rethink intellectual property laws in the context of changes wrought by information technology (Napster-type issues), new global diseases (pharmaceutical issues), and the human genome (who owns the secrets of life?). In other words, the fight against terrorism, as important as it is, cannot subsume the multitude of thorny questions that must be resolved if a global economy is to operate efficiently and humanely.

CEOs in the Siege Economy

The changing context for economic activity — government–business cooperation, globalization rethought and revised, a U.S. foreign policy broadened beyond commercial considerations — raises the question of what specific role American global CEOs ought to play in today's marketplace and society.

In *The Mind of the CEO*, I underscored the intense competitive pressures under which corporate leaders operate, and the difficulty they themselves identify in undertaking broader roles of leadership in society. In the wake of September 11, this tension has become even more acute. The economic climate has deteriorated badly, putting excruciating pressure on many companies' performances. Business leaders' first concerns will be how to manage their operations in a sharply different global environment. They might conclude that even under the best of circumstances, the war against terrorism will be a long one, and that the uncertainty created will require serious adjustments in their operations. Aside from the immediate security concerns, they may rethink everything from the management of their global supply chains (is it wise to rely on just-in-time inventory deliveries when the global logistical system is subject to disruption?) to the pace of their global diversification (should it be slower or faster?). They will need to reevaluate their ability to assess political risk and to engage in contingency and scenario planning, as well as their competence to deal effectively with a government that is edging into a wartime footing (to be sure, companies' Washington offices will become more important).

The public framework for globalization, however, is at a delicate crossroads. It is tempting to say that the job of shaping a sustainable form of globalization belongs to the world's governments. To an extent that's true, but governments alone cannot do the job. They don't have the long-term global perspective, talent, or experience — nor do they touch people in every facet of their daily lives. As the leaders of companies that help shape how people live, what they buy, and what they think, business executives can and should help in the conceptualization of a new paradigm of globalization — and in the execution of policies predicated upon it. CEOs would do well to remember that they are the major champions — perhaps the only true backers at this time — of globalization. If they are not out front supporting a revised, sustainable globalization, no one else will be.

In the short term, President Bush may need a business council, made up of the country's most enlightened CEOs, to meet with him and his cabinet to discuss these kinds of ideas before patterns are too far along to reverse. The administration, focused on the step-by-step escalation of the war on terrorism, cannot do the necessary planning as well by itself. In the end, moreover, a successful foreign policy will require significant cooperation from American firms. They are, after all, the instru-

ments of economic production, investment, and employment, and the source of technological innovation. When it comes to such issues as the environment, labor standards, and human rights — key components of foreign policy these days — the objectives of the U.S. cannot be fully achieved without the reinforcing actions of American companies.

A Different Kind of War

That broader conceptualization of the war against terrorism ought to begin now. During World War II, everything was naturally subordinated to winning the military contest. But even as the war was waged, a parallel effort was made by the U.S. and Great Britain to lay the groundwork for a strengthened global economy. And when the war was over, attention was turned to building what became the Bretton Woods system. More than a billion people now live in peace and prosperity on four continents because of the foresight shown by those leaders in the throes of war.

Today we are fighting a different kind of war. Although today's world economy has not been nearly so disrupted as the 1940s economy was, the antiterrorism campaign will create a host of new and as-yet-unforeseen complications. This may well be the time for the Bush administration to take the lead in launching a rethinking of the ways that the global economy can be strengthened. In this effort, the participation of a number of America's best CEOs ought to be central.

The case for a new model for the world economy rests in part on the reality that economic systems do not exist in a political vacuum. In the 19th century, Britain ruled the seas, and its capital markets and free-trade stance were the linchpins of the world economy. In recent years, the U.S. has been the world's sole superpower, and it too has wielded disproportionate clout over economic globalization. But this latter system was fraying, even before September 11. Something is wrong when we have so many recurring financial crises around the world. Something is wrong when so much seems to depend on the unpredictable spending patterns of American consumers. Now, a new political alignment seems to be emerging. There may be a new recognition that America cannot always act alone. New coalitions are developing among states. New coalitions could be formed among other nonsovereign actors, too — between corporations and environmentalists, for example. An essential aspect of any rethinking of globalization is to factor in the new politics.

Other longer-term issues exist for corporate America, in particular. At a minimum, to contend with the newly recognized pressures of globalization, corporate strategy, leadership development, and management training need to be revised along the following lines:

- Schools and businesses must focus on producing broad-gauged leaders who can run companies that are profitable and progressive agents of change.
- Undergraduate and graduate schools must train business leaders who can understand geopolitics as well as finance and marketing.
- Corporate governance must be reformed to become less CEO-centric, in order to manage the extraordinary and growing complexity inherent in multinational companies today.

I know that there are many views about how long and deep the American campaign against terrorism will be. Many people express skepticism that the U.S. can sustain this unprecedented kind of war. They say that we will be back to near normal in six months or a year. I don't think so, but we are in the realm of conjecture.

Whatever happens, however, we will look at globalization through a different lens. The same channels of transportation and communication that opened the global economy to trade and investment have opened it to terrorism of different forms. We are vulnerable, and vulnerability unchecked will create uncertainty that can undermine economic progress. Unless it can be overturned, an overpowering sense of exposure impedes the spread of democracy, because societies under threat lean away from liberty toward security.

So the big issue is not whether globalization will proceed; it is too powerful to stop. The big issue is, What kind of globalization? What should be the new paradigm, because, one way or another, there will be one? Can we make it safer? Can we make it more humane and hence more attractive to a broader variety of countries? American government and American business leaders both have an enormous stake in the answers. +

Resources

Joel Kurtzman, "An Interview with Rosabeth Moss Kanter," *s+b*, Third Quarter 1999; www.strategy-business.com/press/article/?art=19327&pg=0

John Micklethwait and Adrian Wooldridge, "Globalization Is No Fait Accompli," *s+b*, Third Quarter 2000; www.strategy-business.com/press/article/?art=14536&pg=0

Randall Rothenberg, "Jeffrey E. Garten: The Thought Leader Interview," *s+b*, First Quarter 2001; www.strategy-business.com/press/article/?art=17917&pg=0

Jeffrey E. Garten, *The Mind of the CEO* (Perseus Books/Basic Books, 2001)

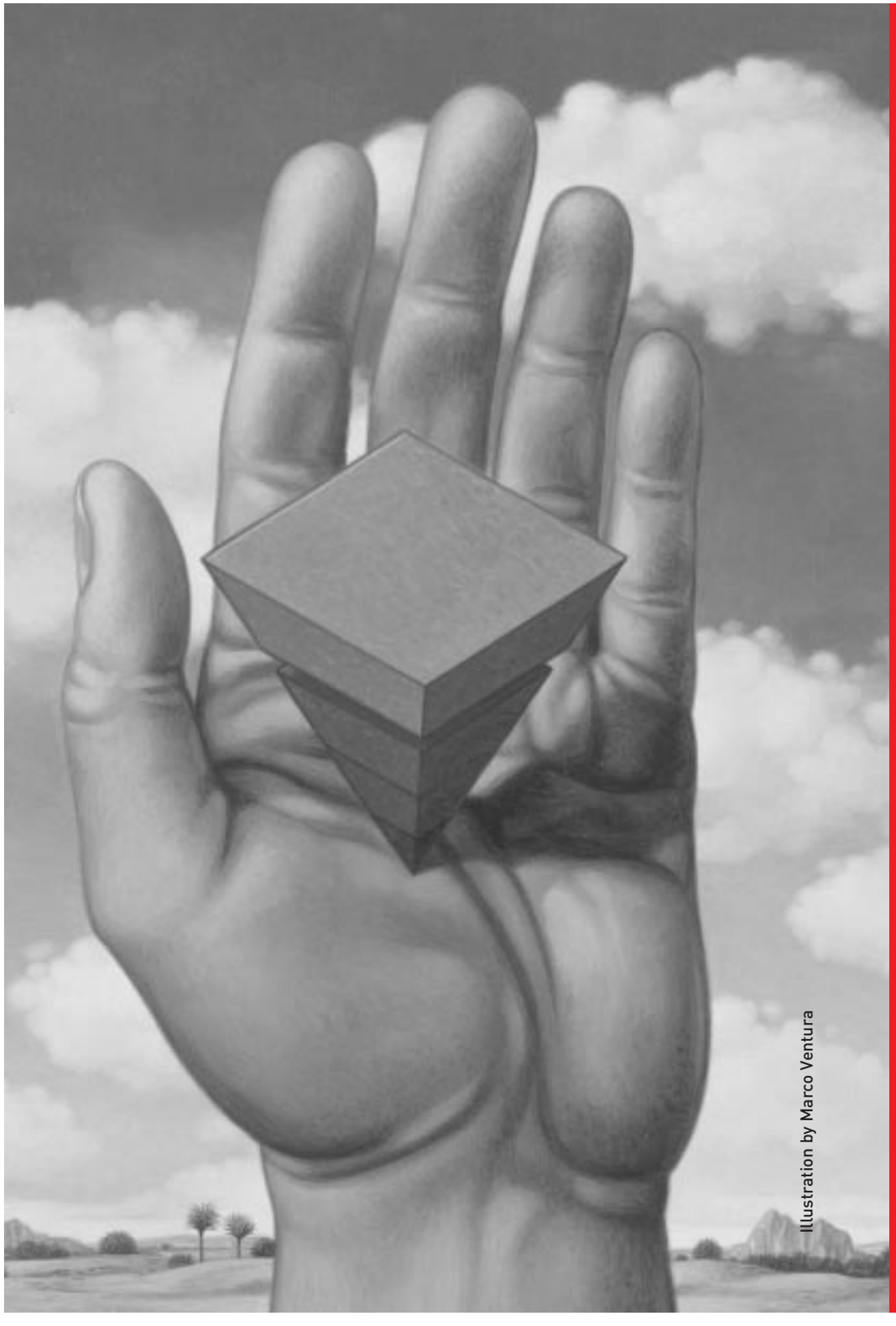


Illustration by Marco Ventura

The Fortune at the Bottom of the Pyramid

The Fortune at the Bottom of the Pyramid

by C.K. Prahalad and Stuart L. Hart

With the end of the Cold War, the former Soviet Union and its allies, as well as China, India, and Latin America, opened their closed markets to foreign investment in a cascading fashion. Although this significant economic and social transformation has offered vast new growth opportunities for multinational corporations (MNCs), its promise has yet to be realized.

First, the prospect of millions of "middle-class" consumers in developing countries, clamoring for products from MNCs, was wildly oversold. To make matters worse, the Asian and Latin American financial crises have greatly diminished the attractiveness of emerging markets. As a consequence, many MNCs worldwide slowed investments and began to rethink risk–reward structures for these markets. This retreat could become even more pronounced in the wake of the terrorist attacks in the United States last September.

The lackluster nature of most MNCs' emerging-market strategies over the past decade does not change the magnitude of the opportunity, which is in reality much larger than previously thought. The real source of market promise is not the wealthy few in the developing world, or even the emerging middle-income consumers: It is the billions of aspiring poor who are joining the market economy for the first time.

This is a time for MNCs to look at globalization strategies through a new lens of inclusive capitalism. For companies with the resources and persistence to compete at the bottom of the world economic pyramid, the prospective rewards include growth, profits, and incalculable contributions to humankind. Countries that still don't have the modern infrastructure or products to meet basic human needs are an ideal testing ground for developing environmentally sustainable technologies and products for the entire world.

Furthermore, MNC investment at "the bottom of the pyramid" means lifting billions of people out of poverty and desperation, averting the social decay, political chaos, terrorism, and environmental meltdown that is certain to continue if the gap between rich and poor countries continues to widen.

Doing business with the world's 4 billion poorest people — two-thirds of the world's population — will require radical innovations in technology and business models. It will require MNCs to reevaluate price–performance relationships for products and services. It will demand a new level of capital efficiency and new ways of measuring financial success. Companies will be forced to transform their understanding of scale, from a "bigger is better" ideal to an ideal of highly distributed small-scale operations married to world-scale capabilities.

In short, the poorest populations raise a prodigious new managerial challenge for the world's wealthiest companies: selling to the poor and helping them improve their lives by producing and distributing products and services in culturally sensitive, environmentally sustainable, and economically profitable ways.

Four Consumer Tiers

At the very top of the world economic pyramid are 75 to 100 million affluent Tier 1 consumers from around the world. (See Exhibit 1.) This is a cosmopolitan group composed of middle- and upper-income people in developed countries and the few rich elites from the developing world. In the middle of the pyramid, in Tiers 2 and 3, are poor customers in developed nations and the rising middle classes in developing countries, the targets of MNCs' past emerging-market strategies.

Now consider the 4 billion people in Tier 4, at the bottom of the pyramid. Their annual per capita income — based on purchasing power parity in U.S. dollars — is less than $1,500, the minimum considered necessary to sustain a decent life. For well

Exhibit 1: **The World Economic Pyramid**

Annual Per Capita Income*	Tiers	Population in Millions
More Than $20,000	1	75–100
$1,500–$20,000	2 & 3	1,500–1,750
Less Than $1,500	4	4,000

* Based on purchasing power parity in U.S.$
Source: U.N. World Development Reports

over a billion people — roughly one-sixth of humanity — per capita income is less than $1 per day.

Even more significant, the income gap between rich and poor is growing. According to the United Nations, the richest 20 percent in the world accounted for about 70 percent of total income in 1960. In 2000, that figure reached 85 percent. Over the same period, the fraction of income accruing to the poorest 20 percent in the world fell from 2.3 percent to 1.1 percent.

This extreme inequity of wealth distribution reinforces the view that the poor cannot participate in the global market economy, even though they constitute the majority of the population. In fact, given its vast size, Tier 4 represents a multitrillion-dollar market. According to World Bank projections, the population at the bottom of the pyramid could swell to more than 6 billion people over the next 40 years, because the bulk of the world's population growth occurs there.

The perception that the bottom of the pyramid is not a viable market also fails to take into account the growing importance of the informal economy among the poorest of the poor, which by some estimates accounts for 40 to 60 percent of all economic activity in developing countries. Most Tier 4 people live in rural villages, or urban slums and shantytowns, and they usually do not hold legal title or deed to their assets (e.g., dwellings, farms, businesses). They have little or no formal education and are hard to reach via conventional distribution, credit, and communications. The quality and quantity of products and services available in Tier 4 is generally low. Therefore, much like an iceberg with only its tip in plain view, this massive segment of the global population — along with its massive market opportunities — has remained largely invisible to the corporate sector.

Fortunately, the Tier 4 market is wide open for technological innovation. Among the many possibilities for innovation, MNCs can be leaders in leapfrogging to products that don't repeat the environmental mistakes of developed countries over the last 50 years. Today's MNCs evolved in an era of abundant natural resources and thus tended to make products and services that were resource-intensive and excessively polluting. The United States' 270 million people — only about 4 percent of the world's population — consume more than 25 percent of the planet's energy resources. To re-create those types of consumption patterns in developing countries would be disastrous.

We have seen how the disenfranchised in Tier 4 can disrupt the way of life and safety of the rich in Tier 1 — poverty breeds discontent and extremism. Although complete income equality is an ideological pipe dream, the use of commercial development to bring people out of poverty and give them the chance for a better life is critical to the stability and health of the global economy and the continued success of Western MNCs.

The Invisible Opportunity

Among the top 200 MNCs in the world, the overwhelming majority are based in developed countries. U.S. corporations dominate, with 82; Japanese firms, with 41, are second, according to a list compiled in December 2000 by the Washington, D.C.–based Institute for Policy Studies. So it is not surprising that MNCs' views of business are conditioned by their knowledge of and familiarity with Tier 1 consumers. Perception of market opportunity is a function of the way many managers are socialized to think and the analytical tools they use. Most MNCs automatically dismiss the bottom of the pyramid because they judge the market based on income or selections of products and services appropriate for developed countries.

To appreciate the market potential of Tier 4, MNCs must come to terms with a set of core assumptions and practices that influence their view of developing countries. We have identified the following as widely shared orthodoxies that must be reexamined:

- **Assumption #1** The poor are not our target consumers because with our current cost structures, we cannot profitably compete for that market.
- **Assumption #2** The poor cannot afford and have no use for the products and services sold in developed markets.
- **Assumption #3** Only developed markets appreciate and will pay for new technology. The poor can use the previous generation of technology.
- **Assumption #4** The bottom of the pyramid is not important to the long-term viability of our business. We can leave Tier 4 to governments and nonprofits.
- **Assumption #5** Managers are not excited by business challenges that have a humanitarian dimension.

Exhibit 2: **Innovation and MNC Implications in Tier 4**

Drivers of Innovation	Implications for MNCs
Increased access among the poor to TV and information	Tier 4 is becoming aware of many products and services and is aspiring to share the benefits
Deregulation and the diminishing role of governments and international aid	More hospitable investment climate for MNCs entering developing countries and more cooperation from nongovernmental organizations
Global overcapacity combined with intense competition in Tiers 1, 2, and 3	Tier 4 represents a huge untapped market for profitable growth
The need to discourage migration to overcrowded urban centers	MNCs must create products and services for rural populations

• **Assumption #6** Intellectual excitement is in developed markets. It is hard to find talented managers who want to work at the bottom of the pyramid.

Each of these key assumptions obscures the value at the bottom of the pyramid. It is like the story of the person who finds a $20 bill on the sidewalk. Conventional economic wisdom suggests if the bill really existed, someone would already have picked it up! Like the $20 bill, the bottom of the pyramid defies conventional managerial logic, but that doesn't mean it isn't a large and unexplored territory for profitable growth. Consider the drivers of innovation and opportunities for companies in Tier 4. (See Exhibit 2.) MNCs must recognize that this market poses a major new challenge: how to combine low cost, good quality, sustainability, and profitability.

Furthermore, MNCs cannot exploit these new opportunities without radically rethinking how they go to market. Exhibit 3 suggests some (but by no means all) areas where an entirely new perspective is required to create profitable markets in Tier 4.

Tier 4 Pioneers

Hindustan Lever Ltd. (HLL), a subsidiary of Great Britain's Unilever PLC and widely considered the best-managed company in India, has been a pioneer among MNCs exploring markets at the bottom of the pyramid. For more than 50 years, HLL has served India's small elite who could afford to buy MNC products. In the 1990s, a local firm, Nirma Ltd., began offering detergent products for poor consumers, mostly in rural areas. In fact, Nirma created a new business system that included a new product formulation, low-cost manufacturing process, wide distribution network, special packaging for daily purchasing, and value pricing.

Exhibit 3: **New Strategies for the Bottom of the Pyramid**

Price Performance	Views of Quality
• Product development • Manufacturing • Distribution	• New delivery formats • Creation of robust products for harsh conditions (heat, dust, etc.)
Sustainability	**Profitability**
• Reduction in resource intensity • Recyclability • Renewable energy	• Investment intensity • Margins • Volume

HLL, in typical MNC fashion, initially dismissed Nirma's strategy. However, as Nirma grew rapidly, HLL could see its local competitor was winning in a market it had disregarded. Ultimately, HLL saw its vulnerability and its opportunity: In 1995, the company responded with its own offering for this market, drastically altering its traditional business model.

HLL's new detergent, called Wheel, was formulated to substantially reduce the ratio of oil to water in the product, responding to the fact that the poor often wash their clothes in rivers and other public water systems. HLL decentralized the production, marketing, and distribution of the product to leverage the abundant labor pool in rural India, quickly creating sales channels through the thousands of small outlets where people at the bottom of the pyramid shop. HLL also changed the cost structure of its detergent business so it could introduce Wheel at a low price point.

Exhibit 4: **Nirma vs. HLL in India's Detergent Market (1999)**

	Nirma	HLL (Wheel)	HLL (High-End Products)
Total Sales ($ Million)	150	100	180
Gross Margin (%)	18	18	25
ROCE (%)	121	93	22

Source: Presentation by John Ripley, senior vice president, Unilever, at the Academy of Management Meeting, August 10, 1999

Today, Nirma and HLL are close competitors in the detergent market, with 38 percent market share each, according to IndiaInfoline.com, a business intelligence and market research service. Unilever's own analysis of Nirma and HLL's competition in the detergent business reveals even more about the profit potential of the marketplace at the bottom of the pyramid. (See Exhibit 4.)

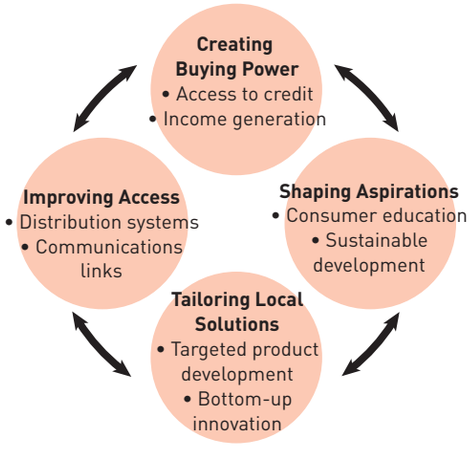
Contrary to popular assumptions, the poor can be a very profitable market — especially if MNCs change their business models. Specifically, Tier 4 is not a market that allows for the traditional pursuit of high margins; instead, profits are driven by volume and capital efficiency. Margins are likely to be low (by current norms), but unit sales can be extremely high. Managers who focus on gross margins will miss the opportunity at the bottom of the pyramid; managers who innovate and focus on economic profit will be rewarded.

Nirma has become one of the largest branded detergent makers in the world. Meanwhile, HLL, stimulated by its emergent rival and its changed business model, registered a 20 percent growth in revenues per year and a 25 percent growth in profits per year between 1995 and 2000. Over the same period, HLL's market capitalization grew to $12 billion — a growth rate of 40 percent per year. HLL's parent company, Unilever, also has benefited from its subsidiary's experience in India. Unilever transported HLL's business principles (not the product or the brand) to create a new detergent market among the poor in Brazil, where the Ala brand has been a big success. More important, Unilever has adopted the bottom of the pyramid as a corporate strategic priority.

As the Unilever example makes clear, the starting assumption must be that serv-

ing Tier 4 involves bringing together the best of technology and a global resource base to address local market conditions. Cheap and low-quality products are not the goal. The potential of Tier 4 cannot be realized without an entrepreneurial orientation: The real strategic challenge for managers is to visualize an active market where only abject poverty exists today. It takes tremendous imagination and creativity to engineer a market infrastructure out of a completely unorganized sector.

Exhibit 5: **The Commercial Infrastructure at the Bottom of the Pyramid**



Serving Tier 4 markets is not the same as serving existing markets better or more efficiently. Managers first must develop a commercial infrastructure tailored to the needs and challenges of Tier 4. Creating such an infrastructure must be seen as an investment, much like the more familiar investments in plants, processes, products, and R&D.

Further, contrary to more conventional investment strategies, no firm can do this alone. Multiple players must be involved, including local governmental authorities, nongovernmental organizations (NGOs), communities, financial institutions, and other companies. Four elements — creating buying power, shaping aspirations, improving access, and tailoring local solutions — are the keys to a thriving Tier 4 market. (See Exhibit 5.)

Each of these four elements demands innovation in technology, business models, and management processes. And business leaders must be willing to experiment, collaborate, empower locals, and create new sources of competitive advantage and wealth.

Creating Buying Power

According to the International Labor Organization's *World Employment Report 2001*, nearly a billion people — roughly one-third of the world's work force — are either underemployed or have such low-paying jobs that they cannot support themselves or their families. Helping the world's poor elevate themselves above this desperation line is a business opportunity to do well and do good. To do so effectively, two interventions are crucial — providing access to credit, and increasing the earning potential of the poor. A few farsighted companies have already begun to blaze this trail with startlingly positive results.

Commercial credit historically has been unavailable to the very poor. Even if those living in poverty had access to a bank, without collateral it is hard to get credit from the traditional banking system. As Peruvian economist Hernando de Soto demonstrates in his pathbreaking work, *The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else*, commercial credit is central to building a market economy. Access to credit in the U.S. has allowed people of modest means to systematically build their equity and make major purchases, such as houses, cars, and education.

The vast majority of the poor in developing countries operate in the "informal" or extralegal economy, since the time and cost involved in securing legal title for their assets or incorporation of their microenterprises is prohibitive. Developing countries have tried governmental subsidies to free the poor from the cycle of poverty, with little success. Even if the poor were able to benefit from government support to start small businesses, their dependence on credit from local moneylenders charging usurious rates makes it impossible to succeed. Local moneylenders in Mumbai, India, charge interest rates of up to 20 percent per day. This means that a vegetable vendor who borrows Rs.100 ($2.08) in the morning must return Rs.120 ($2.50) in the evening.

Extending credit to the poor so they can elevate themselves economically is not a new idea. Consider how I.M. Singer & Company, founded in 1851, provided credit as a way for millions of women to purchase sewing machines. Very few of those women could have afforded the steep $100 price tag, but most could afford a payment of $5 per month.

The same logic applies on a much larger scale in Tier 4. Consider the experience of the Grameen Bank Ltd. in Bangladesh, one of the first in the world to apply a microlending model in commercial banking. Started just over 20 years ago by Muhammad Yunus, then a professor in the Economics Department at Chittagong University, Bangladesh, Grameen Bank pioneered a lending service for the poor that has inspired thousands of microlenders, serving 25 million clients worldwide, in developing countries and wealthy nations, including the United States and Great Britain.

Grameen Bank's program is designed to addresses the problems of extending credit to lowest-income customers — lack of collateral, high credit risk, and contractual enforcement. Ninety-five percent of its 2.3 million customers are women, who, as the traditional breadwinners and entrepreneurs in rural communities, are better credit risks than men. Candidates for loans must have their proposals thoroughly evaluated and supported by five nonfamily members of the community. The bank's sales and service people visit the villages frequently, getting to know the women who have loans

and the projects in which they are supposed to invest. In this way, lending due diligence is accomplished without the mountain of paperwork and arcane language common in the West.

With 1,170 branches, Grameen Bank today provides microcredit services in more than 40,000 villages, more than half the total number in Bangladesh. As of 1996, Grameen Bank had achieved a 95 percent repayment rate, higher than any other bank in the Indian subcontinent. However, the popularity of its services has also spawned more local competitors, which has cut into its portfolio and shrunk its profits over the past few years.

In addition, Grameen Bank's rate of return is not easy to assess. Historically, the bank was an entirely manual, field-based operation, a structure that undercut its efficiency. Today, spin-offs such as Grameen Telecom (a provider of village phone service) and Grameen Shakti (a developer of renewable energy sources) are helping Grameen Bank build a technology infrastructure to automate its processes. As the bank develops its online business model, profitability should increase dramatically, highlighting the importance of information technology in the acceleration of the microcredit revolution.

Perhaps the most pertinent measure of Grameen Bank's success is the global explosion of institutional interest in microlending it has stimulated around the world. In South Africa, where 73 percent of the population earns less than R5,000 ($460) per month, according to a 2001 World Bank study, retail banking services for low-income customers are becoming one of the most competitive and fast-growing mass markets. In 1994, Standard Bank of South Africa Ltd., Africa's leading consumer bank, launched a low-cost, volume-driven e-banking business, called AutoBank E, to grow revenue by providing banking services to the poor. Through the use of 2,500 automated teller machines (ATMs) and 98 AutoBank E-centres, Standard now has the largest presence in South Africa's townships and other under-serviced areas of any domestic bank. As of April 2001, Standard served nearly 3 million low-income customers and is adding roughly 60,000 customers per month, according to South Africa's *Sunday Times*.

Standard does not require a minimum income of customers opening an AutoBank E account, although they must have some regular income. People who have never used a bank can open an account with a deposit of as little as $8. Customers are issued an ATM card and shown how to use it by staff who speak a variety of African dialects. A small flat fee is charged for each ATM transaction. An interest-bearing "savings purse" is attached to every account to encourage poor customers to save. Interest rates on deposits are low, but superior to keeping cash in a jar. The *Sunday Times* also reported that Standard Bank is considering a loan program for low-income clients.

Computerization of microlending services not only makes the overall operation more efficient, but also makes it possible to reach many more people — lending money to individuals with no collateral and no formal address. Since there is lower overhead and little paperwork, AutoBank's costs are 30 to 40 percent lower than those at traditional branches.

At the 1999 Microcredit Summit, the United Nations, in conjunction with several major MNCs, such as Citigroup Inc. and Monsanto Company, set a goal of making basic credit available to the 100 million poorest families in the world by the year 2005. Unfortunately, the success of this undertaking has been slowed by high transaction costs, a lack of automation, and poor information and communications infrastructures in rural areas.

To address these issues and accelerate the development of microlending, French banker Jacques Attali, the founding president of the European Bank for Reconstruction and Development and a former chief aide of French President François Mitterand during the 1980s, has created PlaNet Finance. Its Web site, www.planetfinance.org, links thousands of microcredit groups worldwide into a network to help microbanks share solutions and lower costs.

Ultimately, the development of an automated solution for tracking and processing the millions of small loans associated with microlending should be possible. If processing and transaction costs can be reduced enough, they can then be bundled together and sold in the secondary market to multinational financial institutions like Citigroup. This would greatly expand the capital available for microlending beyond the current pool from donors and governments.

In the United States, microlending has also taken root over the past decade in poor urban neighborhoods. For example, the ShoreBank Corporation, formerly South Shore Bank, has demonstrated the profitability of banking for the poor in Chicago's troubled South Side. Project Enterprise, a Grameen-like program based in New York City, is aimed at minority entrepreneurs.

Several multinational banks are beginning to offer microbanking services in developing countries. Citigroup, for instance, is experimenting in Bangalore, India, with 24/7 services for customers with as little as a $25 on deposit. Initial results are very positive.

Shaping Aspirations

Sustainable product innovations initiated in Tier 4, and promoted through consumer education, will not only positively influence the choices of people at the bottom of the pyramid, but may ultimately reshape the way Americans and others in Tier 1 live. Indeed, in 20 years, we may look back to see that Tier 4 provided the early market pull

for disruptive technologies that replaced unsustainable technologies in developed countries and advanced the fortunes of MNCs with foresight.

For example, Unilever's HLL subsidiary has tackled the lack of practical, inexpensive, low-energy-consuming refrigeration in India. HLL's laboratories developed a radically different approach to refrigeration that allows ice cream to be transported across the country in standard nonrefrigerated trucks. The system allows quantum reductions in electricity use and makes dangerous and polluting refrigerants unnecessary. As a bonus, the new system is cheaper to build and use.

Electricity, water, refrigeration, and many other essential services are all opportunities in developing countries. A U.S.-based NGO, the Solar Electric Light Fund (SELF), has creatively adapted technology and applied microcredit financing to bring electrical service to people in remote villages in Africa and Asia who otherwise would spend money to burn hazardous kerosene, candles, wood, or dung for their light and cooking. SELF's rural electrification system is based on small-scale on-site power generation using renewable resources. A revolving loan fund gives villagers the financial means to operate these electrical systems themselves, also creating jobs. Since its founding in 1990, SELF has launched projects in China, India, Sri Lanka, Nepal, Vietnam, Indonesia, Brazil, Uganda, Tanzania, South Africa, and the Solomon Islands.

The success of SELF and other NGOs focused on small-scale distributed energy solutions has begun to attract the attention of Western companies such as the U.S.'s Plug Power Inc. (fuel cells) and Honeywell Inc. (microturbines). They see the logic in moving into a wide-open market in Tier 4 rather than trying to force their technology prematurely into applications for the developed markets, where incumbents and institutions stand in their way. With several billion potential customers around the world, investments in such innovations should be well worth it.

Improving Access

Because Tier 4 communities are often physically and economically isolated, better distribution systems and communication links are essential to development of the bottom of the pyramid. Few of the large emerging-market countries have distribution systems that reach more than half of the population. (Hence the continued dependence of the poorest consumers on local products and services and moneylenders.) As a consequence, few MNCs have designed their distribution systems to cater to the needs of poor rural customers.

Creative local companies, however, lead the way in effective rural distribution. In India, for instance, Arvind Mills has introduced an entirely new delivery system for blue jeans. Arvind, the world's fifth-largest denim manufacturer, found Indian domestic denim sales limited. At $40 to $60 a pair, the jeans were not affordable to the masses, and the existing distribution system reached only a few towns and villages. So Arvind introduced "Ruf & Tuf" jeans — a ready-to-make kit of jeans components (denim, zipper, rivets, and a patch) priced at about $6. Kits were distributed through a network of thousands of local tailors, many in small rural towns and villages, whose self-interest motivated them to market the kits extensively. Ruf & Tuf jeans are now the largest-selling jeans in India, easily surpassing Levi's and other brands from the U.S. and Europe.

MNCs can also play a role in distributing the products of Tier 4 enterprises in Tier 1 markets, giving bottom-of-the-pyramid enterprises their first links to international markets. Indeed, it is possible through partnerships to leverage traditional knowledge bases to produce more sustainable, and in some cases superior, products for consumption by Tier 1 customers.

Anita Roddick, CEO of The Body Shop International PLC, demonstrated the power of this strategy in the early 1990s through her company's "trade not aid" program of sourcing local raw material and products from indigenous people.

More recently, the Starbucks Corporation, in cooperation with Conservation International, has pioneered a program to source coffee directly from farmers in the Chiapas region of Mexico. These farms grow coffee beans organically, using shade, which preserves songbird habitat. Starbucks markets the product to U.S. consumers as a high-quality, premium coffee; the Mexican farmers benefit economically from the sourcing arrangement, which eliminates intermediaries from the business model. This direct relationship also improves the local farmers' understanding and knowledge of the Tier 1 market and its customer expectations.

Information poverty may be the single biggest roadblock to sustainable development. More than half of humanity has yet to make a single phone call. However, where telephones and Internet connections do exist, for the first time in history, it is possible to imagine a single, interconnected market uniting the world's rich and poor in the quest for truly sustainable economic development. The process could transform the "digital divide" into a "digital dividend."

Ten years ago, Sam Pitroda, currently chairman and CEO of London-based Worldtel Ltd., a company created by a telecommunications union to fund telecom development in emerging markets, came to India with the idea of "rural telephones." His original concept was to have a community telephone, operated by an entrepreneur (usually a woman) who charged a fee for the use of the telephone and kept a percentage as wages for maintaining the telephone. Today, from most parts of India, it is possible to call anyone in the world.

Other entrepreneurs have introduced fax services, and some are experimenting

with low-cost e-mail and Internet access. These communication links have dramatically altered the way villages function and how they are connected to the rest of the country and the world. With the emergence of global broadband connections, opportunities for information-based business in Tier 4 will expand significantly.

New ventures such as CorDECT in India and Celnicos Communications in Latin America are developing information technology and business models suited to the particular requirements of the bottom of the pyramid. Through shared-access models (e.g., Internet kiosks), wireless infrastructure, and focused technology development, companies are dramatically reducing the cost of being connected. For example, voice and data connectivity typically costs companies $850 to $2,800 per line in the developed world; CorDECT has reduced this cost to less than $400 per line, with a goal of $100 per line, which would bring telecommunications within reach of virtually everyone in the developing world.

Recognizing an enormous business and development opportunity, Hewlett-Packard Company has articulated a vision of "world e-inclusion," with a focus on providing technology, products, and services appropriate to the needs of the world's poor. As part of this strategy, HP has entered into a venture with the MIT Media Lab and the Foundation for Sustainable Development of Costa Rica — led by former President Jose Maria Figueres Olsen — to develop and implement "telecenters" for villages in remote areas. These digital town centers provide modern information technology equipment with a high-speed Internet connection at a price that is affordable, through credit vehicles, at the village level.

Bringing such technology to villages in Tier 4 makes possible a number of applications, including tele-education, telemedicine, microbanking, agricultural extension services, and environmental monitoring, all of which help to spur microenterprise, economic development, and access to world markets. This project, named Lincos, is expected to spread from today's pilot sites in Central America and the Caribbean to Asia, Africa, and Central Europe.

Tailoring Local Solutions

As we enter the new century, the combined sales of the world's top 200 MNCs equal nearly 30 percent of total world gross domestic product. Yet these same corporations employ less than 1 percent of the world's labor force. Of the world's 100 largest economies, 51 are economies internal to corporations. Yet scores of Third World countries have suffered absolute economic stagnation or decline.

If MNCs are to thrive in the 21st century, they must broaden their economic base and share it more widely. They must play a more active role in narrowing the gap between rich and poor. This cannot be achieved if these companies produce only so-called global products for consumption primarily by Tier 1 consumers. They must nurture local markets and cultures, leverage local solutions, and generate wealth at the lowest levels on the pyramid. Producing in, rather than extracting wealth from, these countries will be the guiding principle.

To do this, MNCs must combine their advanced technology with deep local insights. Consider packaging. Consumers in Tier 1 countries have the disposable income and the space to buy in bulk (e.g., 10-pound boxes of detergent from superstores like Sam's Club) and shop less frequently. They use their spending money to "inventory convenience." Tier 4 consumers, strapped for cash and with limited living space, shop every day, but not for much. They can't afford to stock up on household items or be highly selective about what they buy; they look for single-serve packaging. But consumers with small means also have the benefit of experimentation. Unburdened by large quantities of product, they can switch brands every time they buy.

Already in India, 30 percent of personal care products and other consumables, such as shampoo, tea, and cold medicines, are sold in single-serve packages. Most are priced at Rs. 1 (about 1¢). Without innovation in packaging, however, this trend could result in a mountain of solid waste. Dow Chemical Company and Cargill Inc. are experimenting with an organic plastic that would be totally biodegradable. Such packaging clearly has advantages in Tier 4, but it could also revolutionize markets at all four tiers of the world pyramid.

For MNCs, the best approach is to marry local capabilities and market knowledge with global best practices. But whether an initiative involves an MNC entering Tier 4 or an entrepreneur from Tier 4, the development principles remain the same: New business models must not disrupt the cultures and lifestyles of local people. An effective combination of local and global knowledge is needed, not a replication of the Western system.

The development of India's milk industry has many lessons for MNCs. The transformation began around 1946, when the Khira District Milk Cooperative, located in the state of Gujarat, set up its own processing plant under the leadership of Verghese Kurien and created the brand Amul, today one of the most recognized in the country.

Unlike the large industrial dairy farms of the West, in India, milk originates in many small villages. Villagers may own only two to three buffaloes or cows each and bring their milk twice a day to the village collection center. They are paid every day for the milk they deliver, based on fat content and volume. Refrigerated vans transport the milk to central processing plants, where it is pasteurized. Railroad cars then transport the milk to major urban centers.

The entire value chain is carefully managed, from the village-based milk produc-

tion to the world-scale processing facilities. The Khira District cooperative provides such services to the farmers as veterinary care and cattle feed. The cooperative also manages the distribution of pasteurized milk, milk powder, butter, cheese, baby food, and other products. The uniqueness of the Amul cooperative is its blending of decentralized origination with the efficiencies of a modern processing and distribution infrastructure. As a result, previously marginal village farmers are earning steady incomes and being transformed into active market participants.

Twenty years ago, milk was in short supply in India. Today, India is the world's largest producer of milk. According to India's National Dairy Development Board, the country's dairy cooperative network now claims 10.7 million individual farmer member–owners, covers 96,000 village-level societies, includes 170 milk-producer unions, and operates in more than 285 districts. Milk production has increased 4.7 percent per year since 1974. The per capita availability of milk in India has grown from 107 grams to 213 grams per day in 20 years.

Putting It All Together

Creating buying power, shaping aspirations, improving access, and tailoring local solutions — the four elements of the commercial infrastructure for the bottom of the pyramid are intertwined. Innovation in one leverages innovation in the others. Corporations are only one of the actors; MNCs must work together with NGOs, local and state governments, and communities.

Yet someone must take the lead to make this revolution happen. The question is, Why should it be MNCs?

Even if multinational managers are emotionally persuaded, it is not obvious that large corporations have real advantages over small, local organizations. MNCs may never be able to beat the cost or responsiveness of village entrepreneurs. Indeed, empowering local entrepreneurs and enterprises is key to developing Tier 4 markets. Still, there are several compelling reasons for MNCs to embark on this course:

• **Resources.** Building a complex commercial infrastructure for the bottom of the pyramid is a resource- and management-intensive task. Developing environmentally sustainable products and services requires significant research. Distribution channels and communication networks are expensive to develop and sustain. *Few local entrepreneurs have the managerial or technological resources to create this infrastructure.*

• **Leverage.** MNCs can transfer knowledge from one market to another — from China to Brazil or India — as Avon, Unilever, Citigroup, and others have demonstrated. Although practices and products have to be customized to serve local needs, *MNCs, with their unique global knowledge base, have an advantage that is not easily accessible to local entrepreneurs.*

• **Bridging.** MNCs can be nodes for building the commercial infrastructure, providing access to knowledge, managerial imagination, and financial resources. Without MNCs as catalysts, well-intentioned NGOs, communities, local governments, entrepreneurs, and even multilateral development agencies will continue to flounder in their attempts to bring development to the bottom. *MNCs are best positioned to unite the range of actors required to develop the Tier 4 market.*

• **Transfer.** Not only can MNCs leverage learning from the bottom of the pyramid, but they also have the capacity to transfer innovations up-market all the way to Tier 1. As we have seen, Tier 4 is a testing ground for sustainable living. *Many of the innovations for the bottom can be adapted for use in the resource- and energy-intensive markets of the developed world.*

It is imperative, however, that managers recognize the nature of business leadership required in the Tier 4 arena. Creativity, imagination, tolerance for ambiguity, stamina, passion, empathy, and courage may be as important as analytical skill, intelligence, and knowledge. Leaders need a deep understanding of the complexities and subtleties of sustainable development in the context of Tier 4. Finally, managers must have the interpersonal and intercultural skills to work with a wide range of organizations and people.

MNCs must build an organizational infrastructure to address opportunity at the bottom of the pyramid. This means building a local base of support, reorienting R&D to focus on the needs of the poor, forming new alliances, increasing employment intensity, and reinventing cost structures. These five organizational elements are clearly interrelated and mutually reinforcing.

• **Build a local base of support.** Empowering the poor threatens the existing power structure. Local opposition can emerge very quickly, as Cargill Inc. found in its sunflower-seed business in India. Cargill's offices were twice burned, and the local politicians accused the firm of destroying locally based seed businesses. But Cargill persisted. Through Cargill's investments in farmer education, training, and supply of farm inputs, farmers have significantly improved their productivity per acre of land. Today, Cargill is seen as the friend of the farmer. Political opposition has vanished.

To overcome comparable problems, MNCs must build a local base of political support. As Monsanto and General Electric Company can attest, the establishment of a coalition of NGOs, community leaders, and local authorities that can counter entrenched interests is essential. Forming such a coalition can be a very slow process. Each player has a different agenda; MNCs have to understand these agendas and create shared aspirations. In China, this problem is less onerous: The local bureaucrats are also the local entrepreneurs, so they can easily see the benefits to their enterprise and their village, town, or province. In countries such as India and Brazil, such align-

ment does not exist. Significant discussion, information sharing, the delineation of benefits to each constituency, and sensitivity to local debates is necessary.

• **Conduct R&D focused on the poor.** It is necessary to conduct R&D and market research focused on the unique requirements of the poor, by region and by country. In India, China, and North Africa, for example, research on ways to provide safe water for drinking, cooking, washing, and cleaning is a high priority. Research must also seek to adapt foreign solutions to local needs. For example, a daily dosage of vitamins can be added to a wide variety of food and beverage products. For corporations that have distribution and brand presence throughout the developing world, such as Coca-Cola Company, the bottom of the pyramid offers a vast untapped market for such products as water and nutritionals.

Finally, research must identify useful principles and potential applications from local practices. In Tier 4, significant knowledge is transmitted orally from one generation to the next. Being respectful of traditions but willing to analyze them scientifically can lead to new knowledge. The Body Shop's creative CEO, Ms. Roddick, built a business predicated on understanding the basis for local rituals and practices. For example, she observed that some African women use slices of pineapple to cleanse their skin. On the surface, this practice appears to be a meaningless ritual. However, research showed active ingredients in pineapple that cleared away dead skin cells better than chemical formulations.

MNCs must develop research facilities in emerging markets such as China, India, Brazil, Mexico, and Africa, although few have made a big effort so far. Unilever is an exception; it operates highly regarded research centers in India, employing more than 400 researchers dedicated to the problems of "India-like markets."

• **Form new alliances.** MNCs have conventionally formed alliances solely to break into new markets; now they need to broaden their alliance strategies. By entering into alliances to expand in Tier 4 markets, MNCs gain insight into developing countries' culture and local knowledge. At the same time, MNCs improve their own credibility. They may also secure preferred or exclusive access to a market or raw material. We foresee three kinds of important relationships: Alliances with local firms and cooperatives (such as the Khira District Milk Cooperative); alliances with local and international NGOs (like Starbucks's alliance with Conservation International in coffee); and alliances with governments (e.g., Merck & Company's recent alliance in Costa Rica to foster rain forest preservation in exchange for bioprospecting rights).

Given the difficulty and complexity of constructing business models dependent on relationships with national or central governments (e.g., large infrastructure development), we envision more alliances at the local and regional level. To succeed in such alliances, MNC managers must learn to work with people who may not have the same agenda or the same educational and economic background as they do. The challenge and payoff is how to manage and learn from diversity — economic, intellectual, racial, and linguistic.

• **Increase employment intensity.** MNCs accustomed to Tier 1 markets think in terms of capital intensity and labor productivity. Exactly the opposite logic applies in Tier 4. Given the vast number of people at the bottom of the pyramid, the production and distribution approach must provide jobs for many, as in the case of Ruf & Tuf jeans from Arvind Mills: It employed an army of local tailors as stockers, promoters, distributors, and service providers, even though the cost of the jeans was 80 percent below that of Levi's. As Arvind demonstrated, MNCs need not employ large numbers of people directly on their payroll, but the organizational model in Tier 4 must increase employment intensity (and incomes) among the poor and groom them to become new customers.

• **Reinvent cost structures.** Managers must dramatically reduce cost levels relative to those in Tier 1. To create products and services the poor can afford, MNCs must reduce their costs significantly — to, say, 10 percent of what they are today. But this cannot be achieved by fine-tuning the current approaches to product development, production, and logistics. The entire business process must be rethought with a focus on functionality, not on the product itself. For example, financial services need not be distributed only through branch offices open from 9 a.m. to 5 p.m. Such services can be provided at a time and place convenient to the poor consumer — after 8 p.m. and at their homes. Cash-dispensing machines can be placed in safe areas — police stations and post offices. Iris recognition used as a security device could substitute for the tedious personal-identification number and card for identification.

Lowering cost structures also forces a debate on ways to reduce investment costs. This will inevitably lead to greater use of information technology to develop production and distribution systems. As noted, village-based phones are already transforming the pattern of communications throughout the developing world. Add the Internet, and we have a whole new way of communicating and creating economic development in poor, rural areas. Creative use of IT will emerge in these markets as a means to dramatically lower the costs associated with access to products and services, distribution, and credit management.

A Common Cause

The emergence of the 4 billion people who make up the Tier 4 market is a great opportunity for MNCs. It also represents a chance for business, government, and civil society to join together in a common cause. Indeed, we believe that pursuing strategies for the bottom of the pyramid dissolves the conflict between proponents of free

trade and global capitalism on one hand, and environmental and social sustainability on the other.

Yet the products and services currently offered to Tier 1 consumers are not appropriate for Tier 4, and accessing this latter market will require approaches fundamentally different from those even in Tiers 2 and 3. Changes in technology, credit, cost, and distribution are critical prerequisites. Only large firms with global reach have the technological, managerial, and financial resources to dip into the well of innovations needed to profit from this opportunity.

New commerce in Tier 4 will not be restricted to businesses filling such basic needs as food, textiles, and housing. The bottom of the pyramid is waiting for high-tech businesses such as financial services, cellular telecommunications, and low-end computers. In fact, for many emerging disruptive technologies (e.g., fuel cells, photovoltaics, satellite-based telecommunications, biotechnology, thin-film microelectronics, and nanotechnology), the bottom of the pyramid may prove to be the most attractive early market.

So far, three kinds of organizations have led the way: local firms such as Amul and Grameen Bank; NGOs such as the World Resources Institute, SELF, The Rainforest Alliance, The Environmental Defense Fund, and Conservation International, among others; and a few MNCs such as Starbucks, Dow, Hewlett-Packard, Unilever, Citigroup, DuPont, Johnson & Johnson, Novartis, and ABB, and global business partnerships such as the World Business Council for Sustainable Business Development. But to date, NGOs and local businesses with far fewer resources than the MNCs have been more innovative and have made more progress in developing these markets.

It is tragic that as Western capitalists we have implicitly assumed that the rich will be served by the corporate sector, while governments and NGOs will protect the poor and the environment. This implicit divide is stronger than most realize. Managers in MNCs, public policymakers, and NGO activists all suffer from this historical division of roles. A huge opportunity lies in breaking this code — linking the poor and the rich across the world in a seamless market organized around the concept of sustainable growth and development.

Collectively, we have only begun to scratch the surface of what is the biggest potential market opportunity in the history of commerce. Those in the private sector who commit their companies to a more inclusive capitalism have the opportunity to prosper and share their prosperity with those who are less fortunate. In a very real sense, the fortune at the bottom of the pyramid represents the loftiest of our global goals. ✚

Resources

The concepts in this article were first articulated in 1998, and have been made available for discussion in a working paper. For more information, contact the authors.

Stuart Hart, "Beyond Greening: Strategies for a Sustainable World," *Harvard Business Review*, January–February 1997; www.hbsp.harvard.edu/hbr/index.html

C.K. Prahalad and Kenneth Lieberthal, "The End of Corporate Imperialism," *Harvard Business Review*, July–August 1998; www.hbsp.harvard.edu/hbr/index.html

"Is the Digital Divide a Problem or an Opportunity?" *Business Week Supplement*, December 18, 2000

Robert Chambers, *Whose Reality Counts? Putting First Last* (ITDG Publishing, 1997)

Thomas L. Friedman, *The Lexus and the Olive Tree: Understanding Globalization* (Farrar, Straus and Giroux, 1999)

Amartya Sen, *Development as Freedom* (Alfred A. Knopf, 1999)

Hernando de Soto, *The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else* (Basic Books, 2000)

War-Game Reports

Bioterrorism: Improving Preparedness and Response
By Gary Ahlquist and Heather Burns
First published by Booz Allen Hamilton, March 2002

Port Security War Game: Implications for U.S. Supply Chains
By Mark Gerencser, Jim Weinberg, and Don Vincent
First published by Booz Allen Hamilton, February 2003

Bioterrorism: Improving Preparedness and Response

Bioterrorism: Improving Preparedness and Response

by Gary Ahlquist and Heather Burns

Government and health-care businesses explored innovative ideas and practical solutions to bioterrorism in a war game. Designed to proactively mobilize the participants to improve our nation's preparedness and response to bioterrorism, the war game was sponsored by Booz Allen Hamilton and The Council for Excellence in Government. The war game highlighted the need for a new kind of public/private partnership in the pursuit of homeland security.

War-gaming is a powerful process for thinking about the future that challenges conventional wisdom and allows participants to break with "known truths" and past assumptions. Top leaders from medical products companies, health-care providers, insurers, and government agencies dealt with choices, dilemmas, and consequences of their actions, and identified next steps to improve real-world coordination, cooperation, and capabilities.

The Scenario

When the unthinkable becomes real, we need new ways of thinking. In the post-September 11 world, more powerful strategic tools must supplement traditional scenario planning, if we are to imagine, and prepare for, the unimaginable.

Imagine this: aerosolized pneumonic plague bacteria are released simultaneously in two major cities in a coordinated terrorist attack. Although initial symptoms resemble flu, plague is nearly 100 percent fatal if not treated early with powerful antibiotics, and, unlike anthrax or West Nile disease, it is highly contagious. The simulated epidemic is unleashed in Detroit, Mich., and Norfolk, Va.

This was the scenario posed to 75 government and health-care professionals in a war game conducted on December 17 and 18, 2001, in Washington D.C. The war game highlighted the need for a new kind of public/private partnership in the pursuit of homeland security.

The bioterrorism war game brought together senior policymakers in the Department of Health and Human Services, the Federal Emergency Management Agency, the Department of Defense, the Department of Veterans Affairs, and state and local government, with business participants, including CEOs and senior executives in medical products companies, including pharmaceuticals and biotechnology, health-care providers, including hospitals, HMOs, and physicians, insurers, and health industry associations.

Booz Allen Hamilton was uniquely positioned to host this exercise, because of our long history of work for both commercial and government clients, our many engagements in government security, and our broad experience in staging war games for government and corporate clients.

Participants learned that communicable bioterrorism is not like natural disasters or epidemics, because it spreads so much more rapidly, and because it can be launched simultaneously in multiple locations. The "worried well" quickly overload the health-care system, and widespread panic stresses law enforcement and other social services to the breaking point. And while the immediate responders are all local, decision making, on such issues as where to distribute drugs and how much, how to educate the public, and when to close borders or airports, quickly becomes national.

This means that the levels of preparation and response in place in our country today are not adequate, but they can be leveraged. The nation can cope with such an attack, but only if we are ready with a response that is quick, coordinated across business and government, well prepared, and thought out ahead of time.

The basic assumption is that the old rules don't apply any more.

Traditionally, neither private industry, nor many government agencies have played an active role in homeland security, which has been almost exclusively the domain of the Department of Defense. But a potential bioterrorist attack would require government agencies, in particular the Department of Health and Human Services, and health-care businesses to play a new national security role.

The War Game

The goal of the war game was to proactively mobilize government and health-care businesses to explore innovative ideas and practical solutions to improve our nation's preparedness and response to bioterrorism. Participants had to deal with choices, dilemmas, and the consequences of their actions, as well as identify next steps to improve real world coordination and capabilities in response to a bioterrorism scenario.

Although health-care executives have discussed the possibility of a bioterrorist attack with government agencies, even before September 11, the war game was an

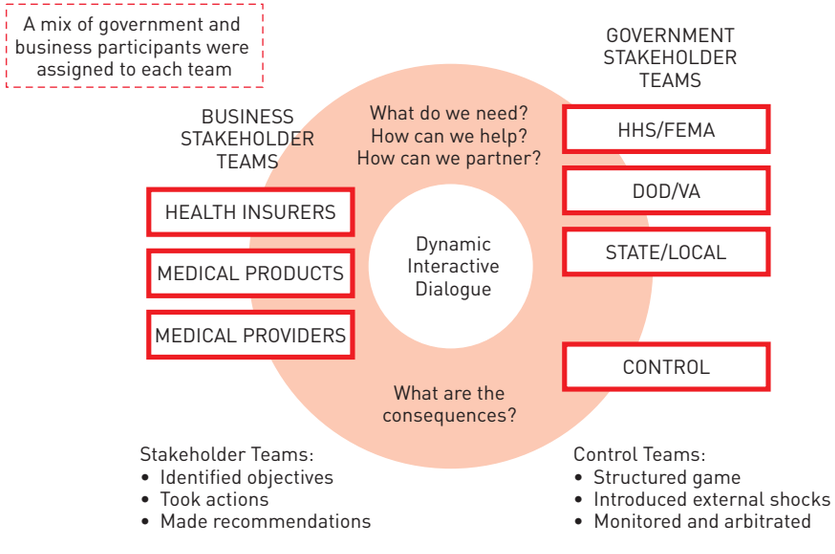
unprecedented meeting of top leaders in these groups in a simultaneous dialogue. Participants were organized into teams representing key business and government sectors, with a mix of government representatives and businesspeople assigned to each team. (See Exhibit 1.) The mixed groups gave individuals a rapid education in how other organizations think and act, as well as providing a first check on ideas and suggestions.

The purpose was not to predict the future, and the simulation was staged with the fervent hope that a bioterrorist attack will never occur. Nor was the intent to assess the preparedness or responsiveness of specific groups, but rather to raise the level of awareness across all participants so that all will be more prepared to respond should a real disaster occur.

The goal was to answer pressing questions for the nation and for their individual organizations:

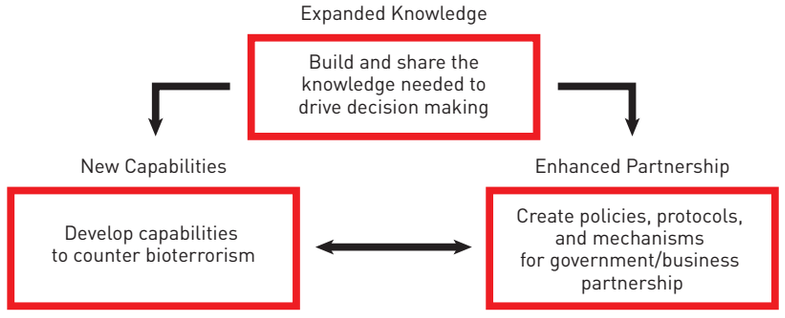
- How should we better prepare for or respond in the event of a future bioterrorist attack?
- How can I bring the unique capabilities of my organization and my sector to bear on the challenges of a bioterrorism attack?
- What is in the minds of other players involved in the response? How does government think about this issue/how do businesses think about this issue?
- What do other players have to offer that will help me respond? What are the implications of the actions of others on my ability to respond and on the overall goals of my organization?
- What are alternative public/private partnership models to enhance our preparedness and response?

Exhibit 1: **Participants were organized into teams representing key business and government sectors**



Source: Booz Allen Hamilton

Exhibit 2: **Teams suggested three major priorities for "their" new national security roles**



Source: Booz Allen Hamilton

Teams observed that a lack of appropriate in-place mechanisms made it difficult to respond to the attack.

Teams discovered that massive, immediate action was required, but they also found that the lack of a common language between government and industry, and the lack of a single point of contact between these groups stymied the rapid movement needed. Participants agreed that new thinking is needed, but many groups at first fell back on established practices and processes that slowed everyone's response.

Government and business teams initially followed a conservative, measured approach, as they struggled to define their roles and understand who to go to for information, direction, and resources. No mechanisms were in place to enable quick coordination across agencies and businesses to mobilize the resources available. Teams concluded that the government alone cannot protect the American people from bioterrorism, so it is essential to mobilize business resources.

Coordination and cooperation across businesses, many of which are competitors, is also required to address the scale of the problem.

Key Learnings

Teams faced several dilemmas in responding to the bioterrorism attack. Clearly the extreme contagiousness of plague, and the lack of a vaccine, called for both quarantine (or "protective isolation") and the rapid and extensive prophylactic treatment of uninfected individuals with antibiotics. But quarantining massive portions of the population raised civil liberties and law enforcement issues with no easy answers, while wide-

spread prophylaxis would strain drug supplies and leave the country vulnerable to new attacks or naturally occurring epidemics. Simple logistics issues, like how to deliver drugs to millions of people, raised seemingly insurmountable obstacles.

Although a myriad of issues presented themselves, they boiled down to four paradoxes:

1. To react quickly, industry needs a single point of contact with the government, but statutes, policies, and programs for dealing with terrorism create multiple points of entry at the interagency and intergovernmental levels.

2. Aggressive containment and prophylaxis can limit the spread of the disease, but moving too quickly might consume reserve capacity needed for future contingencies.

3. Response plans normally focus efforts at the local level, but bioterrorism quickly becomes a national problem, requiring coordination across local, state, and federal governments as well as health-care businesses.

4. Suspending legal, regulatory, and procedural constraints may be necessary to meet immediate needs, but such steps can create serious downstream consequences for public health and business viability.

Lacking prearranged, in-place mechanisms hindered the groups' abilities to cope with these issues. One key learning was that prior planning and practice enables rapid response, which is critical in containing the damage. Mechanisms are needed to collect and share information on pharmaceutical and equipment stockpiles before and during crises. Preparedness will require new levels of communication and cooperation across public/private, local/national, and military/civilian boundaries.

Team Recommendations for Action

At the end of each session, or move, team leaders reported their findings and shared their experiences with other groups. To enable massive immediate action, it is essential that we build and share the knowledge needed to make decisions. Policies, protocols, and mechanisms are needed to coordinate government and business response.

Teams found that the difference between a controlled outbreak and a massive epidemic ultimately hinged on a few key factors. Leadership: Confusion about "who's in charge" in just the first days of the attack had major consequences during the following weeks. Knowledge: Participants agreed that thousands of lives depended on ready information about pharmaceutical and medical equipment stockpiles throughout the nation. Coordination: Individual companies and local governments responded well, but what ultimately mattered was immediate and quick coordination between companies, across agencies and among states.

Building and sharing knowledge means assessing potential actions and their impact. Epidemiological models need to be developed of the top agents, looking at the impact of actions such as quarantine and prophylaxis. Public health readiness can be measured, and a national inventory of medical supplies and other essential materials established. Above all, the information must be shared across government and industry.

This unprecedented sharing requires new policies, protocols, and mechanisms to coordinate government and business response. Response policies must be integrated across federal, state, and local government, and among health-care businesses in order to clarify roles and responsibilities, and to identify the key points of contact and authority. Health-care leaders in government and industry must establish and communicate medical protocols for bioterrorism response. We need new mechanisms for communication, rapid decision making, and coordination of response. These could include the creation of integrated public/private bodies, like the NSTAC/NCS/NCC system for emergency telecommunications.

To enable massive immediate action, it is essential that we build and share the knowledge needed to make decisions.

Clearly, government and business organizations need new capabilities to execute their new roles. Individual companies and agencies could create response plans linked to the overall national plan. Health and Human Services' capability to perform its new national security mission could be enhanced by establishing a crisis action communication system that would link key government and industry players. The government should develop and disseminate a public health threat and response program, in effect, reinventing the old Civil Defense System. Finally, the public health infrastructure must be strengthened at all levels to enable it to execute against homeland security policy.

Conclusion

For the first time ever, the top leaders of government and industry came together in a war game focused on bioterrorism, and perhaps the most salient lesson of the two days was that the public and private sectors must continue to work together to meet this threat.

Public/private partnerships can improve bioterrorism preparation and response by identifying and involving relevant participants; establishing agreed-upon roles and responsibilities; sharing information on stockpiles and surge capacities; predefining economic, legal, and liability parameters and limits; and by coordinating public awareness and education efforts.

Since September 11, security has become a strategic imperative for businesses and organizations of all kinds. Bioterrorism presents unique challenges, in terms of early detection, containment, escalation, response, and recovery.

We believe our December 17–18 war game provided government and industry with a powerful tool to examine and address those challenges. We look forward to continuing the dialogue, and together, to strengthening our nation's security. ✚

Port Security War Game: Implications for U.S. Supply Chains

Port Security War Game: Implications for U.S. Supply Chains

by Mark Gerencser, Jim Weinberg, and Don Vincent

A strategic simulation of a terror attack designed to assess the vulnerability of America's cargo transportation system and supply chains found that such an attack could cripple global trade and have a devastating impact on the nation's economy.

The participants, including leaders from business and government, focused on ways to improve detection before a weapon gets to a U.S. port, as well as strategies to help businesses build resiliency into their operations.

The War Game

The two-day Port Security War Game, sponsored by global management and technology consulting firm Booz Allen Hamilton and The Conference Board, took place on October 2 and 3, 2002, in Washington, D.C., with 85 leaders from a range of government and industry organizations with a critical stake in port security.

Participants from government and private industry were thrust into a mock crisis, an exercise to test how each of these groups would respond to a terrorist attack through the nation's ports.

The war game combined senior policymakers from the Department of Transportation, U.S. Customs, U.S. Coast Guard, Department of Defense, Transportation Security Administration, Office of Homeland Security, intelligence agencies, port authorities, and various other government entities with business participants, including CEOs and senior executives from transportation carriers, technology firms, industry associations, and supply chain representatives of automobile and food/beverage manufacturers and distributors.

Although industry executives had discussed the possibility of a terrorist attack with government agencies even before September 11, the war game was an unprecedented meeting of top leaders in these groups in a simultaneous dialogue.

The goals of the war game were to:

- Mobilize government and businesses to identify and address the challenges of port security;
- Explore innovative ideas and practical solutions to improve our nation's preparedness and response to terrorist disruptions of U.S. ports and supply chains; and
- Discover creative ways to improve preparedness and facilitate cooperation among the organizations and agencies that would need to work together in a real crisis that could completely disrupt the free movement of imports and exports.

The Scenario

The war game examined one of the most disturbing threats to U.S. security — a terrorist attack with "dirty bombs" delivered through one of the millions of cargo containers that enter the country's ports every year.

The scenario began with the accidental discovery of a radiological bomb — conventional explosives wrapped in and designed to scatter radioactive material — in a container on a truck as it left the port of Los Angeles. It escalated with the detention of suspected terrorists at the Port of Savannah. Over a simulated period of three weeks, another bomb was detected in Minneapolis, shipped through Halifax, Nova Scotia, and a third bomb exploded in Chicago.

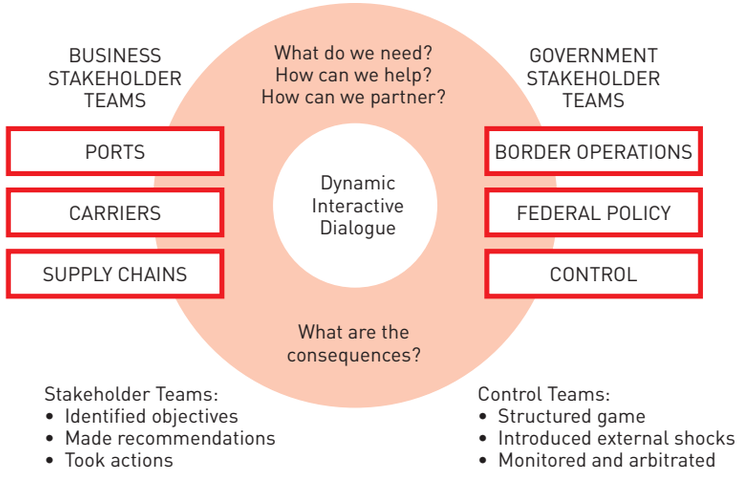
Participants had to react quickly to a crisis with the potential to strangle an economy dependent on the free movement of goods while seeking answers to these questions:

- What are the critical, systemic threats to the nation's port infrastructure?
- How can we ensure port security while maintaining an open and efficient flow of goods through U.S. supply chains?
- How must the public and private sectors work together to enhance the nation's ability to deter and respond to an attack on U.S. transportation systems? How must government agencies cooperate with each other?
- What are the "ripple" implications of a major port closure or container incident on key industry supply chains and their logistics providers?

Participants were organized into teams representing key business and government sectors, with a mix of government representatives and businesspeople assigned to each team. (See Exhibit 1.) The mixed groups gave individuals a rapid education in how other organizations think and act, and also provided a first check on ideas and suggestions.

These teams had to deal with dilemmas, choices, and the consequences of their actions, as well as identify next steps to improve real-world coordination and capa-

Exhibit 1: **Participants Were Organized Into Teams Representing Business and Governmanet Sectors**



Source: Booz Allen Hamilton

bilities in response to the game's scenario.

The purpose was not to predict the future, and the simulation was staged with the fervent hope that a terrorist attack on our ports will never occur. Nor was the intent to assess the preparedness or responsiveness of specific groups, but rather to raise the level of awareness among all participants so that all will be more prepared to respond should a real disaster occur.

Competing Tensions and Choices

Faced with the prospect of an unknown number of radiological weapons entering the U.S. by container, participants found themselves grappling throughout the game with three inherent tensions:

- **Emergency security measures versus their economic impact;**
- **Short-term "quick fixes" (which were not sustainable) versus long-term solutions (which were difficult to implement quickly); and**
- **Homeland security demands versus foreign/trade policy implications.**

For example, the participants discovered that it is easy to close a port in a crisis, but extraordinarily difficult to deal with the unanticipated economic consequences of that closure. In fact, the war game took place against the backdrop of a real-life labor slowdown by West Coast dockworkers, underscoring the critical role ports play in the national economy.

Why a War Game

A war game like the port security exercise exposes ideas that participants don't know they know and solutions that are not apparent on the surface. War-gaming forces people to think differently, to examine the validity of long-held assumptions about how to respond to specific complex or risk situations. By dividing into groups representing the central parties affected by a business crisis and interacting with each other dynamically, under fire, and in a virtual environment, participants experience firsthand the tension and motivations that would exist if the event were real. And by "trying out" this crisis, by living it in a mock setting, they better prepare themselves for how to respond if such a disruption actually occurred.

Out of the war game, new and novel rules inevitably emerge based on the integrated perspective of the participants and the groups they represent. This is a shared innovative vision of the direction that should be pursued in the future for essential organizational imperatives, such as threat protection, early warning, response, business resilience, and business continuity.

Furthermore, participants learned that while multiple authorities had unilateral power to shut down the ports, there was no coordinated means of reopening them and resuming normal operations. Short-term "point solutions" (such as increasing the rate of container inspection upon arrival at port) had limited sustainability. Even on crisis footing, with 24-hour inspections assisted by the National Guard, only 20 percent of incoming containers could be inspected once the ports were reopened. Yet an end-to-end inspection system that would push inspections out to where shipments originated was impossible to implement in a reactionary way.

Long-term solutions will require a rethinking of business and operating models in both the private and public sectors. The ultimate objective is to build resiliency into the global trade system, enhancing the robustness of transportation systems, logistics systems, supply chains, and businesses.

Finally, while securing U.S. ports and borders was an obvious domestic priority, the actions quickly provoked serious foreign policy and international trade policy repercussions.

Participants found that their ultimate decisions — to close two U.S. ports for three days and, as the crisis worsened, all U.S. ports for the nine days thereafter — had a major impact on the economy. Specifically:

- It took approximately three months to clear the container backlog resulting from closings that spanned just 12 days (especially given elevated inspection rates);
- The total cost to the U.S. economy of the closings was $58 billion, including the impact of spoilage, lost sales/contracts, and manufacturing slowdown/halt in production.

Learnings and Recommendations

At specific junctures during the war game, team leaders reported their perspectives and shared their experiences with the other groups. Overwhelmingly, teams reported that to improve global trade resilience, it will be necessary to weave solutions into each step of the supply chain in a layered manner, and response and recovery must be enhanced through coordination of crisis management plans and improved communication among all the participants. No single solution, they agreed, will secure an entire logistics network.

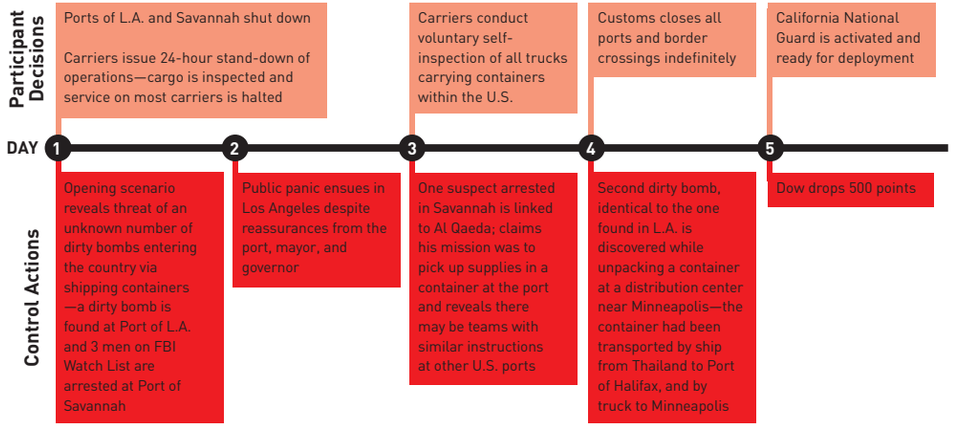
Some of the specific lessons learned included the following:

Security is not just about the ports. The exercise of securing U.S. ports quickly revealed that the larger issue is the vulnerability of today's economy, whose survival is predicated on the free and uninterrupted flow of goods from around the globe. Business and government must embrace security as a strategic and necessary concept in the resilience of a global, interdependent economic system.

Security must be embedded, not "bolted on." Security cannot simply be inserted or applied to existing processes without any sense of whether it is sustainable and scalable. Business strategies and operating models must evolve with robustness embedded in the economics of the industry. Specifically, this means reassessing supply chain strategies to build capabilities that counter disruptions. Manufacturers and retailers, for example, may need to reconsider just-in-time manufacturing, inventory holding practices, and the location of production facilities.

Exhibit 2: **Port Security War Game–Sequence of Events**

Teams, faced with the threat of a terrorist attack against U.S. ports, initially took actions to assess the severity of the situation and secure the transportation network



Source: Booz Allen Hamilton

Point solutions do not work. The process of detection and capture of dangerous materials must begin overseas where goods are loaded and shipped. Options are limited once a container has arrived. Port security must be expanded to involve every link in the chain of delivering goods to market, from origin (manufacturing) through the entire transportation system: sea, highway, rail, and air.

A layering of approaches from origin (loading ports) to the destination (discharge ports) will reduce opportunities to tamper with equipment and cargo and provide multiple checkpoints to ensure the integrity of shipments. International shipping standards, such as preloading container inspection, are a focal point for port safety assurance.

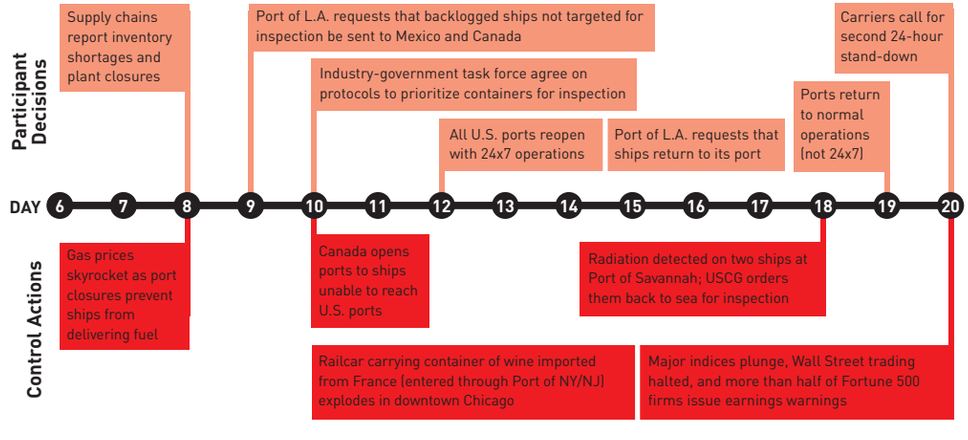
Public-private partnerships are essential. Global trade resiliency in the face of an ambiguous, unceasing terrorist threat requires new solutions and partnerships that only a fully engaged public and private sector can address. Specifically, business and government need to work together in new and perhaps unfamiliar ways to prevent tampering with cargo.

Participants concluded, for example, that international standards are required for preloading container inspections; government must take the lead on this initiative.

Industry leadership, on the other hand, is essential to leverage technology such as GPS tracking devices, e-seals, smart containers, and in-transit radiation detection systems that can enhance the ability to track and monitor the integrity of cargo in transit. At discharge points, national security standards for perimeter control and

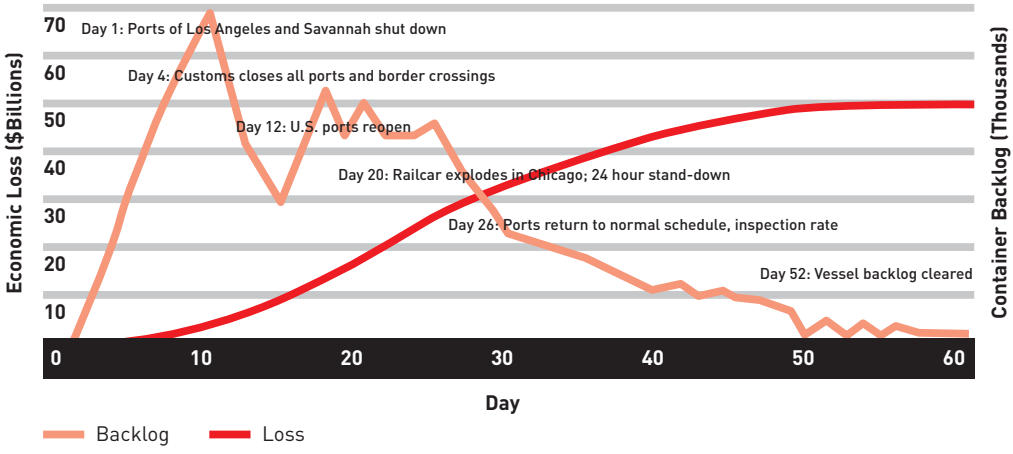
Exhibit 3: **Port Security War Game–Sequence of Events**

Teams then focused on resuming normal operations and mitigating the long-term impact on the economy



Source: Booz Allen Hamilton

Exhibit 4: **Port Security War Game–Economic Impact**



Source: Booz Allen Hamilton

employee credentialing are shared public/private sector responsibilities.

Federal leadership needs to be unified. "We need to overcome organizational inertia and conflicting agendas," said one war-game participant. A single government focal point — be it a department or an official — must be established to effectively deter and detect terrorist events, to oversee response and communications, and to ensure economic recovery.

Final Thoughts

While security has been at the forefront of concerns for the government and businesses alike since September 11, 2001, it has often been addressed in piecemeal fashion (e.g., airline security, cybersecurity). The threat to our supply chains through our transportation network exemplifies the new need for a cohesive, end-to-end public/private partnership.

The intent of the war game was to provide insight into the challenges government and industry face in a world of incomprehensible threats to the economic and geopolitical order. All participants agreed that it served as a foundation for further discussions and for the development of additional concrete preparedness proposals to secure the nation's ports and add resiliency to the nation's supply chains — before an unanticipated crisis occurs. ✚