# Security and Strategy

## in the Age of Discontinuity


## A Management Framework for the Post-9/11 World


by
Ralph W. Shrader
and
Mike McConnell

Photography by
Bruce Weller

**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.

**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.

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



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 inti-

**It is possible to protect ourselves against even the seemingly brutal threats we now face, but it involves far more than installing appropriate technologies.**

mately 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;
- 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.

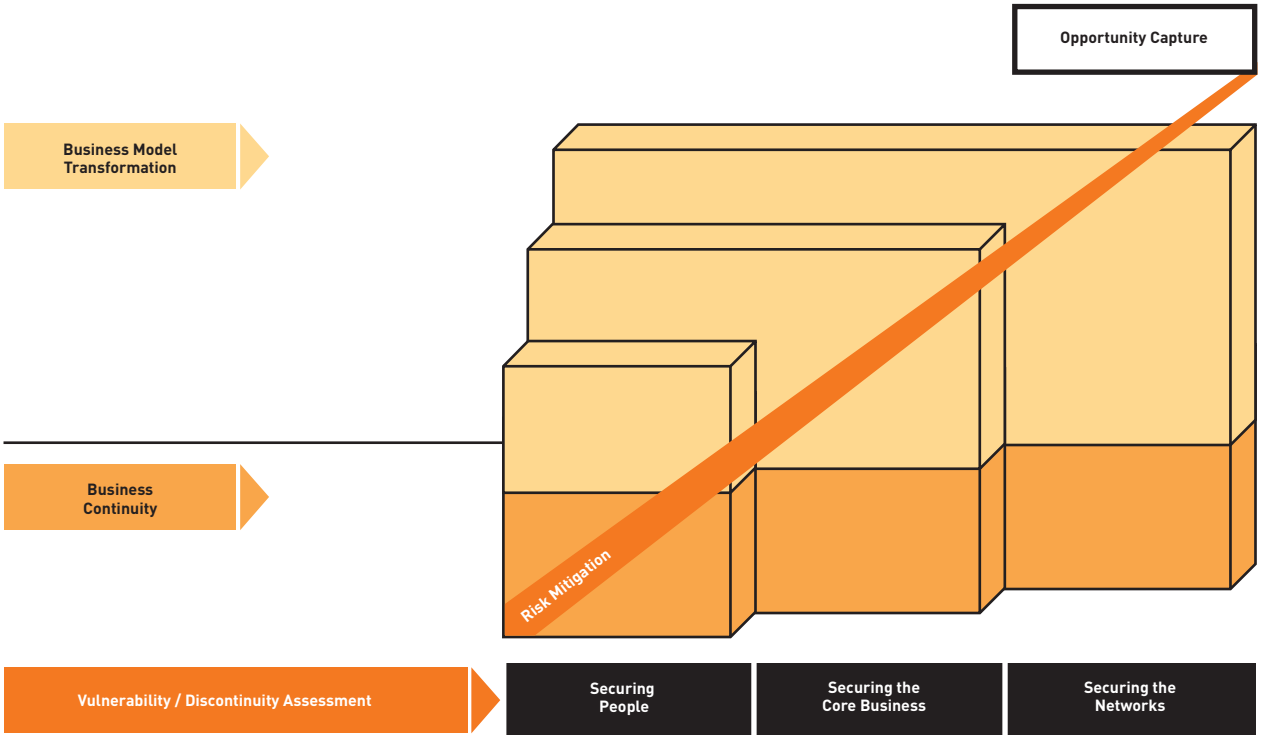
In each stage of this framework, there is both a need for risk mitigation and an opportunity for value capture, which will differ among industries and for individual companies in those industries. Furthermore, a firm must recognize that each stage has both an immediate goal — ensuring business continuity — 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

Exhibit 1: **Strategic Security Management Framework**




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.

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, organiza-

tions 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

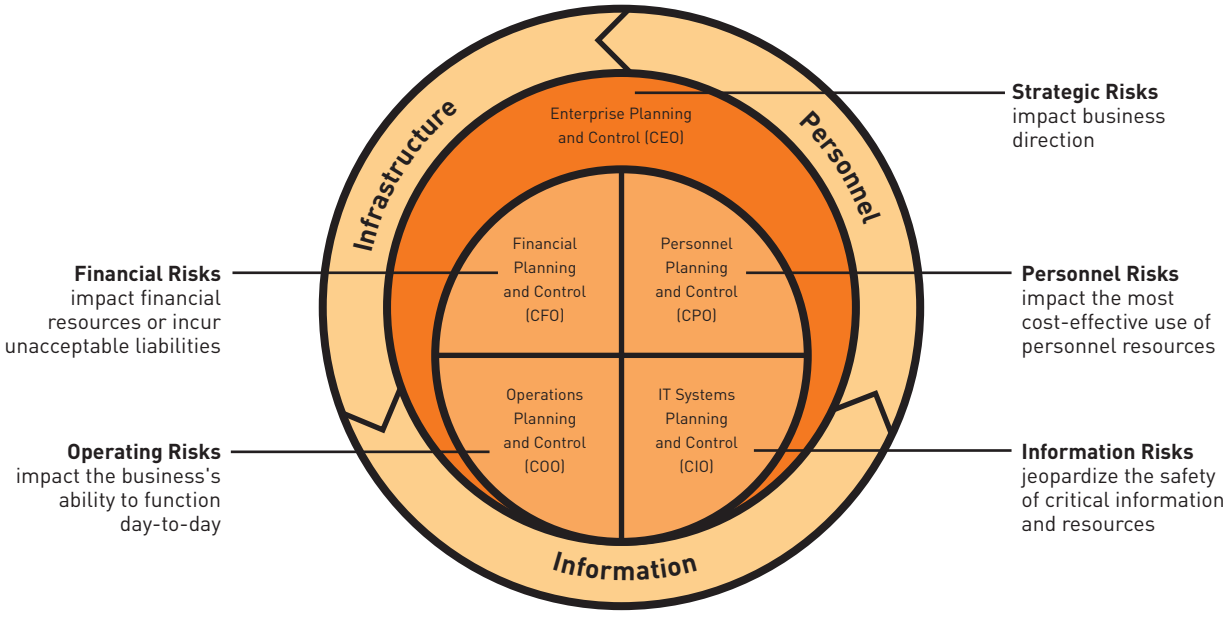
One step beyond securing its people, the company has a responsibility to protect and maintain the continuity of the core business — the systems, facilities, infrastructure, and processes within the reach and control of senior management. Broadly speaking, core-business risks fall into five categories: 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" confer-

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




ence 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,

**Information attack — stealing intelligence, disrupting an infrastructure, or destroying information — could represent a far more serious threat than physical attack.**

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 environment, 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.

# 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,





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

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 wrongminded 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 wargaming helps bring these outcomes to light.

**—R.W.S. and M.M.**





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," above.) 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

**A network of alliances is potentially more resilient than a collection of global acquisitions. But such a network is also a substantial interdependence risk.**

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. +

Reprint No. 02104

## 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.bah.com

"Wargaming: Exploring the Future of Defense," May 2001; www.bah.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)