

by

Mark Gerencser  
gerencser\_mark@bah.com

Jim Weinberg  
weinberg\_jim@bah.com

Don Vincent  
vincent\_don@bah.com

# Port Security War Game

Implications for U.S. Supply Chains

# Port Security War Game

## Implications for U.S. Supply Chains

---

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 October 2–3, 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, millions of which 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?

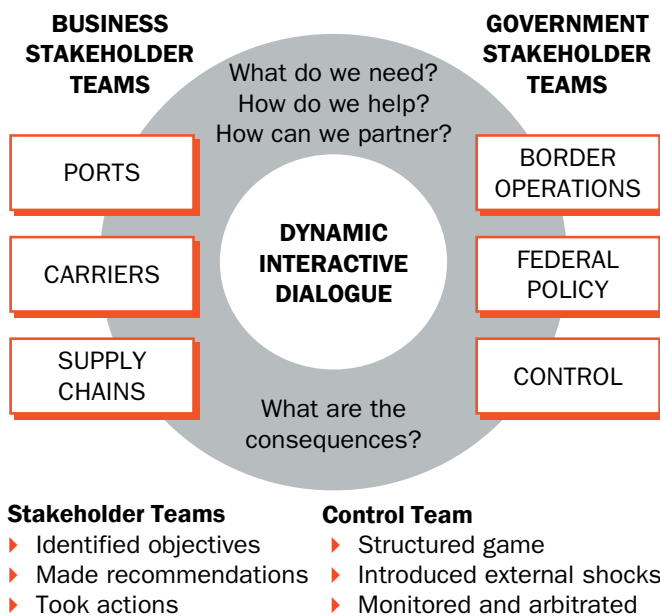
- ▶ How can we ensure port security while maintaining an open and efficient flow of goods through U.S. supply chains?
- ▶ How must the public and private sectors work together to enhance the nation's ability to deter and respond to an attack on U.S. transportation systems? How must government agencies 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 and business people 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.

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 capabilities in response to the game's scenario.

#### Exhibit 1

Participants Were Organized Into Teams Representing Business and Government Sectors



Source: Booz Allen Hamilton

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.

Furthermore, participants learned that while multiple authorities had unilateral power to shut down a port, 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% 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 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.

#### ***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 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 wargame 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 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, cyber security). 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.

## Why a War Game

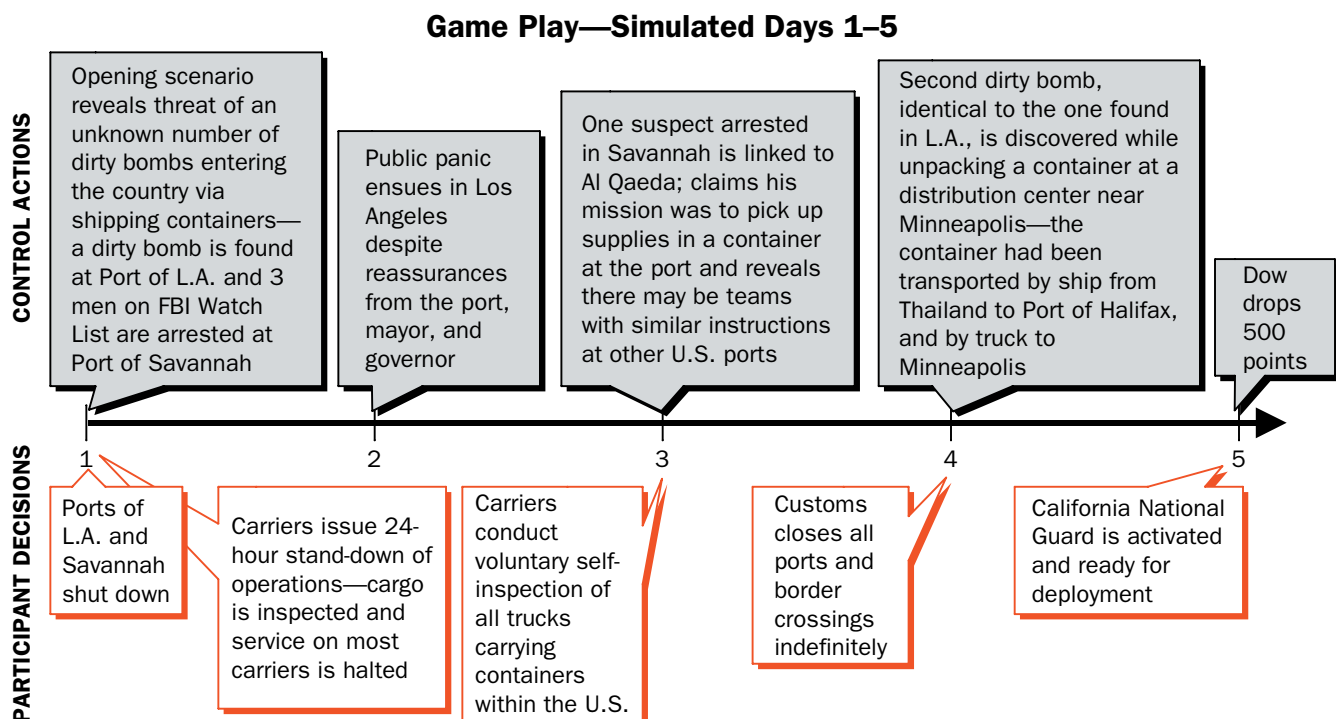
A war game like the port security exercise exposes ideas that participants don't know they know and solutions that are not apparent on the surface. Wargaming forces people to think differently, to examine the validity of long-held assumptions about how to respond to specific complex or risk situations. 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.

## PORT SECURITY WAR GAME—SEQUENCE OF EVENTS

### Exhibit 2

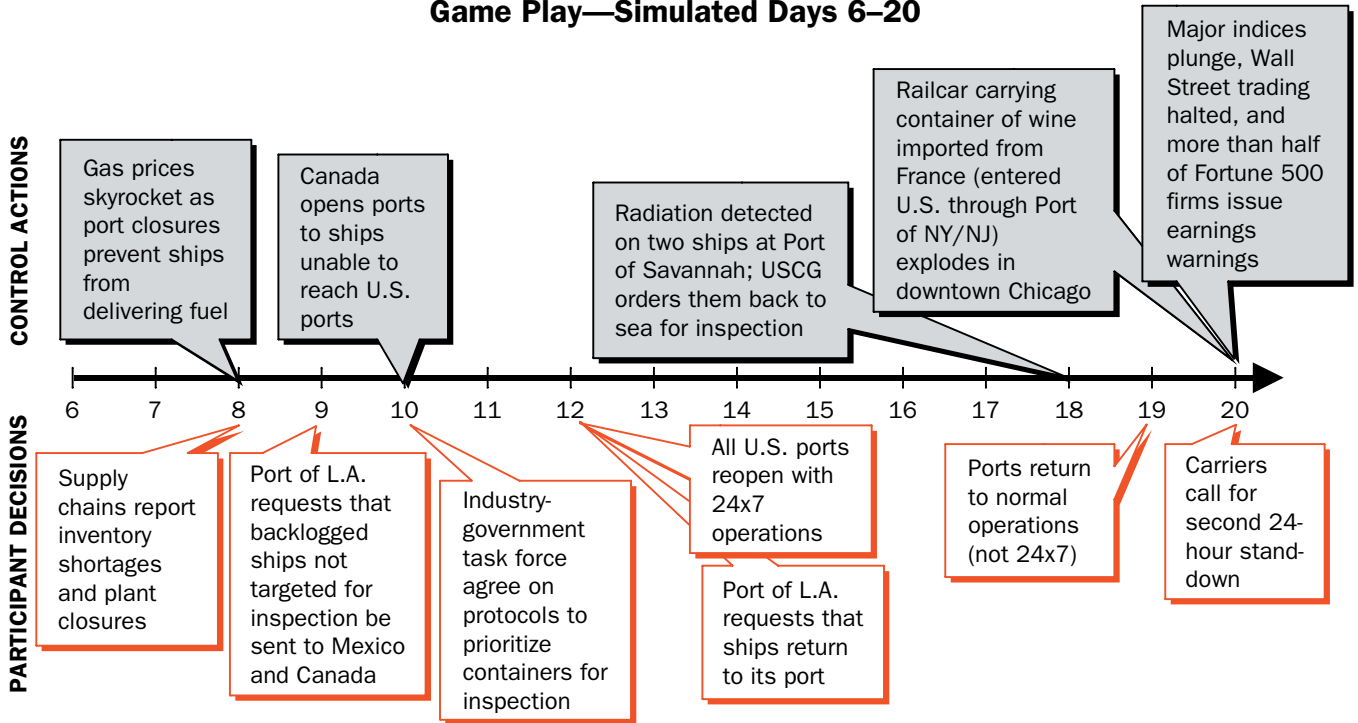
Teams, faced with the threat of a terrorist attack against U.S. ports, initially took actions to assess the severity of the situation and secure the transportation network.



**Exhibit 3**

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

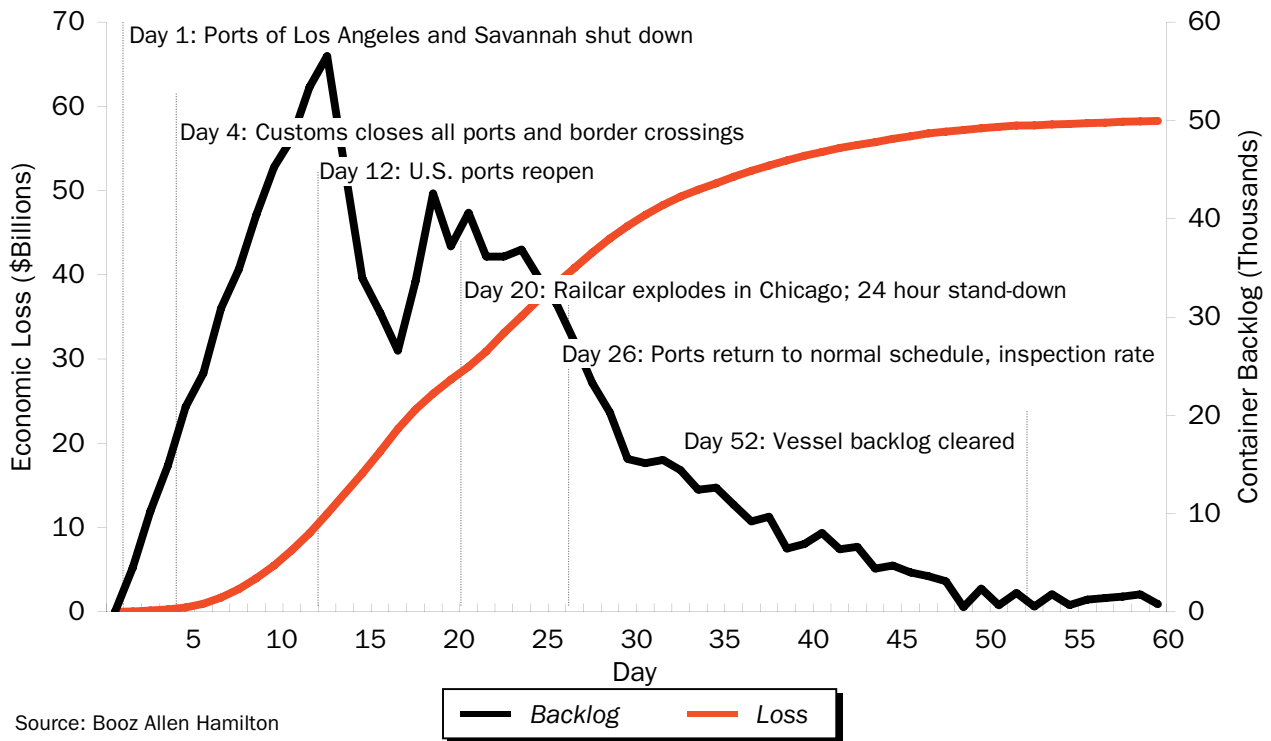
**Game Play—Simulated Days 6–20**



Source: Booz Allen Hamilton

**PORT SECURITY WAR GAME—ECONOMIC IMPACT**

**Exhibit 4**



Source: Booz Allen Hamilton

## What Booz Allen Brings

Booz Allen Hamilton has been at the forefront of management consulting for businesses and governments for more than 80 years. Booz Allen combines strategy with technology and insight with action, working with clients to deliver results today that endure tomorrow.

With over 11,000 employees on six continents, the firm generates annual sales of \$2 billion. Booz Allen provides services in strategy, organization, operations, systems, and technology to the world's leading corporations, government and other public agencies, emerging growth companies, and institutions.

To learn more about the firm, visit the Booz Allen Web site at [www.boozallen.com](http://www.boozallen.com). To learn more about the best ideas in business, visit [www.strategy-business.com](http://www.strategy-business.com), the Web site for **strategy+business**, a quarterly journal sponsored by Booz Allen.

### Booz Allen Global Assurance Campaign

Our nation is profoundly dependent on the critical infrastructures that are predominantly owned and operated by the private sector. Government and business leaders have an obligation to create new public-private partnerships to protect our economy and our industries. Resilient organizations align their strategy, operations, management systems, and decision support capabilities to enable them to uncover, adapt to, and improve their responsiveness to disruptions—for the government, the issue is mission; for industry, the issue is earnings consistency. As this war game showed, together, government and industry can enhance the resilience of global trade. The Global Assurance Team provides enterprise resilience services to businesses, and homeland security consulting services to the U.S. federal and local governments.

**Mark Gerencser** is a Senior Vice President of Booz Allen Hamilton, specializing 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. He can be reached in McLean, Virginia, at 703-902-3082 or [gerencser\\_mark@bah.com](mailto:gerencser_mark@bah.com).

**Jim Weinberg** is a Senior Vice President of Booz Allen Hamilton in our Chicago office and assists companies in step-change improvement in operations performance through implementing new operating models and

technologies. Mr. Weinberg is a co-leader of Booz Allen Hamilton's Enterprise Resilience practice which is forging new frameworks for managing risk in today's dynamic and network-centric business environment. He can be reached in our Chicago office at 312-578-4767 or [weinberg\\_jim@bah.com](mailto:weinberg_jim@bah.com)

**Don Vincent** is a Vice President of Booz Allen Hamilton, specializing in counter-terrorism, 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. He can be reached in Falls Church, Virginia, at 703-289-5153 or [vincent\\_don@bah.com](mailto:vincent_don@bah.com).

## Contact Information

### Vice Presidents

DeAnne Aguirre	415-627-3330
Don Busson	619-725-6575
Mark Gerencser	703-902-3082
Natalie Givans	703-902-7106
Mark Herman	703-902-5986
Chris Kelly	703-377-4301
Gary Lynch	212-551-6587
Joe Mahaffee	301-543-4439
Mike McConnell	973-630-6752
Don Vincent	703-289-5153
Jim Weinberg	312-578-4767
Rich Wilhelm	703-289-5060
Jim Woolsey	703-377-0809

### Principals

Karen Avery	973-630-6904
Mike Delurey	703-289-5277
Dave Jerome	703-289-5280
Jim Newfrock	973-630-6789
Ken Saenz	703-377-0792
Rich Saunders	703-289-5092
Randy Starr	212-551-6558
Dale Watson	703-289-5139

Downloadable digital versions of this article and other Booz Allen Hamilton publications are available from [www.boozallen.com](http://www.boozallen.com).

## Worldwide Offices

<b>Abu Dhabi</b> Charles El-Hage 971-2-6-270882	<b>Buenos Aires</b> Alejandro Stengel 54-1-14-131-0400	<b>Göteborg</b> Bengt Johannesson 46-31-725-93-00	<b>Malmö</b> Ingemar Bengtson 46-40-690-31-00	<b>Paris</b> Panos Cavoulacos 33-1-44-34-3131	<b>Stockholm</b> Kenny Palmberg 46-8-506-190-00
<b>Amsterdam</b> Peter Mensing 31-20-504-1900	<b>Caracas</b> José Gregorio Baquero 58-212-285-3522	<b>Helsinki</b> Kari Iloranta 358-9-61-54-600	<b>McLean</b> Martin J. Bollinger 703-902-3800	<b>Philadelphia</b> Molly Finn 267-330-7900	<b>Sydney</b> Tim Jackson 61-2-9321-1900
<b>Atlanta</b> Joe Garner 404-659-3600	<b>Chicago</b> Gary Ahlquist 312-346-1900	<b>Hong Kong</b> Reg Boudinot 852-2634-1878	<b>Melbourne</b> Tim Jackson 61-3-9221-1900	<b>Rio de Janeiro</b> Paolo Pigorini 55-21-2237-8400	<b>Tampa</b> Joe Garner 813-281-4900
<b>Bangkok</b> Tim Jackson 66-2-653-2255	<b>Cleveland</b> Les Moeller 216-696-1900	<b>Houston</b> Joe Quoyeser 713-650-4100	<b>Mexico City</b> Alonso Martinez 52-55-9178-4200	<b>Rome</b> Fernando Napolitano 39-06-69-20-73-1	<b>Tokyo</b> Eric Spiegel 81-3-3436-8600
<b>Beirut</b> Charles El-Hage 961-1-336433	<b>Colorado Springs</b> Glen Bruels 719-597-8005	<b>Jakarta</b> Ian Buchanan 6221-577-0077	<b>Miami</b> Alonso Martinez 305-670-8050	<b>San Diego</b> Foster Rich 619-725-6500	<b>Vienna</b> Helmut Meier 43-1-518-22-900
<b>Berlin</b> Rene Perillieux 49-30-88705-0	<b>Copenhagen</b> Kenny Palmberg 45-3393-36-73	<b>Lexington Park</b> Neil Gillespie 301-862-3110	<b>Milan</b> Enrico Strada 390-2-72-50-91	<b>San Francisco</b> Bruce Pasternack 415-391-1900	<b>Warsaw</b> Reg Boudinot 48-22-630-6301
<b>Bogotá</b> Jaime Maldonado 57-1-628-5050	<b>Dallas</b> Tim Blansett 214-746-6500	<b>London</b> Peter Bertone 44-20-7393-3333	<b>Munich</b> Richard Hauser 49-89-54525-0	<b>Santiago</b> Alejandro Stengel 562-290-0500	<b>Wellington</b> Tim Jackson 64-4-915-7777
<b>Boston</b> John Harris 617-428-4400	<b>Düsseldorf</b> Thomas Kuenstner 49-211-38900	<b>Los Angeles</b> Tom Hansson 310-348-1900	<b>New York</b> David Knott 212-697-1900	<b>São Paulo</b> Leticia Costa 55-11-5501-6200	<b>Zurich</b> Jens Schädler 41-1-20-64-05-0
<b>Brisbane</b> Tim Jackson 61-7-3230-6400	<b>Frankfurt</b> Rainer Bernnat 49-69-97167-0	<b>Madrid</b> Mercedes Mostajo 34-91-5220606	<b>Oslo</b> Haakon Bjertnaes 47-23-11-39-00	<b>Seoul</b> Jong Chang 82-2-2170-7500	