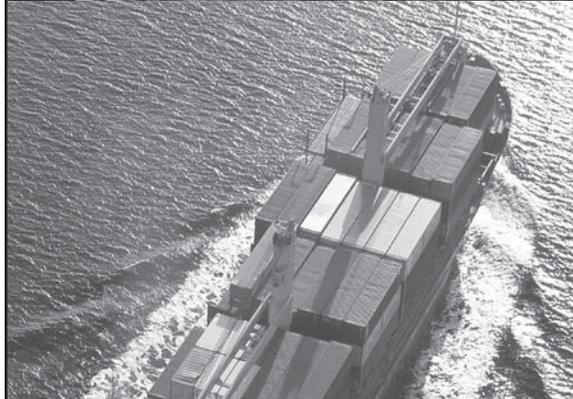


# Investing in Supply Chain Security: Collateral Benefits

Special Report Series



James B. Rice, Jr.  
Director, Integrated Supply Chain  
Management Program  
Center for Transportation and Logistics  
Massachusetts Institute of Technology

Philip W. Spayd  
Research Affiliate  
Center for Transportation and Logistics  
Massachusetts Institute of Technology

IBM Center for  
**The Business  
of Government**



SPECIAL REPORT SERIES

# **Investing in Supply Chain Security: Collateral Benefits**

**James B. Rice, Jr.**

Director, Integrated Supply Chain  
Management Program  
Center for Transportation and Logistics  
Massachusetts Institute of Technology

**Philip W. Spayd**

Research Affiliate  
Center for Transportation and Logistics  
Massachusetts Institute of Technology

May 2005

IBM Center for  
**The Business  
of Government**

# TABLE OF CONTENTS

<b>Foreword</b> .....	3
<b>Executive Summary</b> .....	4
<b>Introduction</b> .....	6
About the Report .....	6
Global Supply Chain Vulnerability and Security .....	6
Making the Case for Supply Chain Security Investments .....	7
<b>Collateral Benefits: A Promising Approach to ROI</b> .....	8
The Major Collateral Benefit: Facilitating Trade .....	8
Options to Create Additional Collateral Benefits .....	9
Collateral Benefits from Asset Visibility and Tracking .....	9
Collateral Benefits from Personnel Security .....	10
Collateral Benefits from Physical Security .....	10
Collateral Benefits from Standards Development .....	10
Collateral Benefits from Supplier Selection and Investment .....	12
Collateral Benefits from Transportation and Conveyance Security .....	12
Collateral Benefits from Building Organizational Infrastructure Awareness and Capabilities .....	12
Collateral Benefits from Collaboration Among Supply Chain Parties .....	13
Collateral Benefits from Proactive Technology Investments .....	14
Collateral Benefits from TQM Investments .....	14
Collateral Benefits from Voluntary Security Compliance .....	15
<b>Achieving Collateral Benefits</b> .....	18
Connecting Security Investments and Collateral Benefits .....	18
Making the Connection: Collateral Benefits Linkage Maps .....	18
Challenges and Choices for Creating Collateral Benefits .....	19
<b>Conclusion</b> .....	21
Observations and Issues to Consider .....	21
The Challenge and Opportunity .....	21
Looking Ahead .....	22
<b>Appendix: Overview of Supply Chain Security Investment Options</b> ....	24
<b>Endnotes</b> .....	26
<b>About the Authors</b> .....	28
<b>Key Contact Information</b> .....	30

## F O R E W O R D

May 2005

On behalf of the IBM Center for The Business of Government, we are pleased to present this report, “Investing in Supply Chain Security: Collateral Benefits,” by James B. Rice, Jr., and Philip W. Spayd. This report is believed to be the first to examine whether the benefits gained from investing in security exceed the costs. It also looks at the important question of whether greater collaboration between government and the private sector leads to improved supply chain security, reduces overall cost, and improves efficiencies.

This is the second comprehensive report that IBM has sponsored to investigate supply chain security. In 2004, the IBM Center for The Business of Government partnered with Michigan State University to publish “Enhancing Security Throughout the Supply Chain,” aimed at helping businesses better understand the threat to supply chains from disruptions. This new report asserts that while the United States and other governments have taken steps to secure international transportation systems, supply chains remain vulnerable to terrorist attack and exposed to the introduction of unauthorized people or weapons. It also responds to industry concern that government action to impose tougher standards and processes erodes trade efficiency by adding cost and complexity.

Rice and Spayd say they approached this report with the objective of encouraging business executives, researchers, and government officials to ask questions, conduct research, and make decisions about how to approach investing in supply chain security to best determine the collateral benefits. They say it is difficult to quantify how a specific security action prevented a problem from occurring in the supply chain or the cost that was avoided. If something is stolen or there is a noticeable reduction in theft, then it can be measured. But calculating the cost of a security breach or disruption that did not occur is virtually impossible.

In this report, Rice and Spayd help business leaders and security managers quantify the business case for increasing investment in security. The report discusses investments in supply chain security that have shown promise to create collateral benefits, as well as emerging benefits that need to be considered. The authors believe that perhaps the most significant collateral benefit is a firm’s ability to continue operations in the event of a disruption to its supply chain, maintaining supply chain continuity with its suppliers and customers wherever it does business.

This report covers many of today’s supply chain security challenges and highlights issues governments and businesses face as they ponder supply chain security investment strategies. And it offers advice on how to use investments in new security programs to improve the efficiency, flexibility, and resilience of the supply chain.

We trust this report will be a catalyst for leadership and fresh thinking, and more research and learning, by the public and private sectors to sustain global supply chain security. We are making progress, but there is still much to do.

Paul Lawrence  
Partner-in-Charge  
IBM Center for The Business of Government  
paul.lawrence@us.ibm.com

Theo Fletcher  
Vice President, Supply Chain Compliance,  
Security and Diversity  
IBM Integrated Supply Chain  
theo@us.ibm.com

## EXECUTIVE SUMMARY

The unthinkable is that a weapon of mass destruction is smuggled through the trade and transportation system via an unsuspecting company's supply chain into a country that is the target of international terrorism. The potential short- and long-term damage in terms of life and economic activity is unfathomable and incalculable. We know that free markets are the targets of terrorists. Osama Bin Laden has said so himself. The United States and other governments have taken steps to secure the international transportation systems and international supply chains. However, because of the worldwide reach of international trade and the sheer number of the components of trade transactions, the systems remain vulnerable to an attack by terrorists on the systems themselves or to being used to introduce a weapon of mass destruction (WMD) or other implement of catastrophic terrorism into the target nation. The danger of a terrorist attack involving the international transportation system remains high. An attack could take place anywhere in the world and would have impact well beyond the location of the attack.

Because of the reach and complexity of the international supply chain, it is difficult for governments to mandate and achieve increased supply chain security through traditional regulatory methods. It is nearly impossible to design security regulations that can rationally improve security throughout the wide range of activities that constitute international trade. Regulations governing security and movements through international supply chains add cost and complexity to the systems. The modern supply chain is already a complex and interrelated network involving the movement of goods, services, funds, and information among a wide range of participants. A real danger is that government actions may be well intended yet may actually diminish trade effi-

ciency without achieving genuine improvements in supply chain security.

Any government with a stake in international trade that stands by without taking measures to improve the security of international trade imposes enormous risks on its citizens and its economy. Neither can businesses afford to do nothing to protect their employees, their company, their customers, and the public from the use of their supply chains to launch a terrorist attack.

Government and business managers also need to be aware of their personal responsibility in protecting international supply chains. An attack launched through a supply chain could damage the credibility and political interests of a government. In this situation, private sector officials, in a legal and social environment of holding corporate officials personally liable for the actions of their firms, could be deemed responsible should their firm's supply chain be compromised. The reputation of the government, the firm, and the individual executives could be irredeemably damaged. A key question, then, is: Can the government and private sector collaborate in a way that achieves substantial improvements in supply chain security and enables private sector firms to reduce their overall cost and improve efficiency?

This leads to a discussion of the collateral benefits that may flow to the firm from investments in security. That is, are there benefits to a firm in addition to the improvements in security that exceed the costs of investment in security? From the perspective of the public sector, can voluntary programs be created that are aimed at maximizing the collateral benefits that firms might achieve as a result of compliance with the program requirements? Might the development

of collateral benefits serve as a catalyst to improve the safety of the public and to bring greater visibility and efficiency in the operation of supply chains?

There has been a great deal of speculation in this area, but there is very little data. Our work is intended to build a framework for executives, researchers, and government officials to ask questions, conduct research, and make decisions about how to approach investments in supply chain security. Firms that derive collateral benefits from investments in security may very well have a competitive advantage over firms that invest in security but do not do so in a way that creates collateral benefits. Governments that create voluntary public/private partnerships that enhance security, maximizing the opportunity for firms to achieve collateral benefits, may achieve higher degrees of improvements in security with lower costs to the governments and the firms.

There needs to be a warning label that comes with the pursuit of collateral benefits: Not all collateral benefits accrue to a firm automatically from investments in security. As noted in this report, the creation of collateral benefits relates to a variety of factors, including the firm's approach to risk management and supply chain security and how it determines its investment options and builds linkages from security to other benefits in the operation of the supply chain. The next steps from a business perspective are to develop the metrics to gauge the actual relationship between the investment in security and the return on the investment, and from a research perspective to capture the necessary data to document the actual dynamics associated with identifying and capturing collateral benefits. Government officials may use this research to develop approaches to trade and transportation security that increase security, protect the public, and provide a platform for increased efficiency within international supply chains.

Looking into the future, perhaps the most significant collateral benefit of investments in security is the development of a firm's ability to continue operations—supply chain continuity—so that it may maintain its economic livelihood in the face of a significant disruption. This entails the ability to achieve dynamic processes for managing the firm's supply chains and the ability to respond quickly and with resilience to changes in the external environ-

ment, irrespective of the nature of the disruption. That will be the dominion of forward-looking companies that plan to operate successfully in a very unstable environment.

# Introduction

## About the Report

This report expands on the emerging concept of collateral benefits derived from making supply chain security (SCS) investments. While this is not a new concept in theory, it is one that is new in practice, and to date there are limited citations of organizations deriving collateral benefits from SCS investments. The good news, however, is that there is increasing evidence and logic that supports the likelihood that meaningful benefits are created from prudent SCS investments.

A key goal in this focused report is to help managers think clearly about the security issues they face within their supply chains. In addition, it should help them consider how investments in increased security might achieve other beneficial results for the company, and how governments, working through the regulatory process and creating public/private partnerships, can enhance supply chain security.

In covering collateral benefits from supply chain security investments, the report focuses on supply chain security investments that have shown promise to create collateral benefits. While a more comprehensive assessment of supply chain security return on investment (ROI) would be useful, this work covers the aspect that represents newly emerging benefits that should be considered when building a business case for making supply chain security investments.

The report utilizes data from an ongoing research initiative at MIT called “Supply Chain Response to Terrorism,” which included several sets of semi-structured interviews with senior supply chain and security leaders from global shippers and carrier

firms operating global supply chains. Although the interviews were conducted in the United States, the firms provided a global perspective given the worldwide nature of their supply chains.

## Global Supply Chain Vulnerability and Security

Business managers throughout the world have recently become sensitized to the vulnerability of their supply chains to an ever-increasing range of security breaches and disruptions that affect global supply chains. Many point to the terrorist attacks on September 11, 2001, but closer analysis reveals a recent series of security breaches and disruptions that threaten national security for many nations. The October 2002 U.S. west coast longshoremen’s lock-out, utility failures in the U.S. and Europe in 2003, the Madrid bombing, and the tsunami in 2004 all illustrate the inherent vulnerability that exists in global supply chains, and the global scope and scale of impact.

Consider the value of international trade to the world economy together with the global supply chains that are delivering the trade, and one can recognize how our economies are especially vulnerable to disruptions, whether they are from a terrorist attack, a natural disaster, an infrastructure failure, or a business collapse. These principles drive the basis for a “new normalcy” in international trade where security plays an increasingly critical role, and entails not only physical security of the supply chain but the ability of firms and nations to continue trading in the face of the security vulnerabilities, previously noted as supply chain continuity.<sup>1</sup>

## Making the Case for Supply Chain Security Investments

With a clear need for increased security in global supply chains, firms are tasked to make appropriate supply chain security investments<sup>2</sup> to protect their assets and operations. Yet, a unique characteristic about security investments is that they defy many traditional methods of calculating ROI if firms only consider cost avoidance.

Security investments by their nature do not directly increase revenues but are intended to prevent costs—when effective, supply chain security measures prevent disruptions, supply chain security breaches, product adulteration, and brand/franchise destruction. In most cases, it is difficult at best to prove that a specific action prevented a problem from occurring, much less how frequently the problem would occur or the costs that were prevented. Aside from theft reduction, where there is tangible evidence of improvements when loss levels are reduced, one cannot measure the cost of a security breach or disruption that did not occur. Ironically, only when a security measure fails can one calculate the cost of the loss for that particular incident.

Theoretically, one could better understand and predict the cost impact of security breaches by studying security breaches and the subsequent costs and losses on a broad, industry-wide scale. Such data could be used to create a probability distribution function that approximates a predictable set of losses across industry. Sadly, this data is not widely available for various reasons, mostly because firms believe that they expose themselves to additional costs and risks by sharing this data. Sharing their loss data and experiences opens up the firm to additional risks: Exposing the loss data may make security weaknesses more evident to the general public, which may result in further losses; exposing actual losses may lead to higher insurance premiums as insurers would adjust premiums to more accurately reflect the higher loss levels; firms may fear reduced access to capital if exposing loss data causes negative public perception of their operations.

As one industrial executive noted, the benefits of security investments are often in the form of avoiding losses, saying “nobody gets credit for solving

problems that did not happen,”<sup>3</sup> as suggested previously. The benefits are difficult to measure if the avoided costs are not incurred. This reflects a challenge to the business to identify and value real savings from avoiding a security breach. Some progress has been made quantifying the benefit from preventing supply chain disruptions, but more work is needed to make the same progress quantifying the benefits of preventing supply chain security breaches.

With these fundamental constraints, business leaders and security managers have had limited success quantifying the business case to fund desirable security investments, leaving supply chains knowingly vulnerable.

An emerging and more powerful way of viewing return on investment for supply chain security investments entails considering more than just cost avoidance benefits. Some firms are recognizing the potential to extend beyond cost avoidance benefits to actually capture cost reduction and efficiency improvements from those same investments. These may be possible by considering the impact of these investments on supply chain operations, and subsequently designing those operations to leverage the investments for process improvement. Those firms pursuing this approach have begun to identify and enjoy collateral benefits of their investments.

### Acronyms & Abbreviations

<b>ACS</b>	Automated Commercial System
<b>CBP</b>	U.S. Customs and Border Protection
<b>C-TPAT</b>	U.S. Customs-Trade Partnership Against Terrorism
<b>GPS</b>	Global Positioning Systems
<b>OS&amp;D</b>	Overages, Shortages, and Damages
<b>RFID</b>	Radio Frequency Identification
<b>ROI</b>	return on investment
<b>SCS</b>	supply chain security
<b>TQM</b>	Total Quality Management

# Collateral Benefits: A Promising Approach to ROI

One promising approach for building a business case for supply chain security lies in the possibility that supply chain security investments may provide valuable benefits in other areas in the firm, and vice versa. These “collateral benefits” (also known as indirect or “dual benefits”) can possibly enhance a business case to increase the return on investment for firms interested in reducing their vulnerability.

At this time, the data on actual collateral benefits resulting from SCS investments is sparse. To date, little work has been done to understand the various aspects and issues associated with creating collateral benefits, although some<sup>4</sup> have recognized the existence and value of creating these collateral benefits.

Firms need to develop economic justifications for their investments in making the supply chain secure and resilient; understanding the dynamics and issues related to creating collateral benefits may provide a valuable investment incentive to justify those investments. Just as Phil Crosby believed that quality investments provide collateral benefits that offset the investments in quality, so too we suggest the possibility that security investments may generate collateral benefits that may exceed the cost of the security investments. Will we find that “security is free”?<sup>5</sup>

## The Major Collateral Benefit: Facilitating Trade

Perhaps the most important potential collateral benefit that may develop from making security system improvements is in facilitating trade. While a primary intention of the investments noted is to make the supply chain secure, by virtue of making the

supply chain secure it becomes less prone to disruption. In some cases, it also helps the supply chain become more capable of withstanding and bouncing back from a disruption.

While this may seem intuitive and a non-starter, only when one considers the potential loss from not being able to trade does one begin to appreciate the impact. Using the U.S. west coast longshoremen’s lockout of 2002 as an example, the economic impact on the U.S. economy has been estimated at between \$10 billion and \$20 billion—this for a 10-day lockout of only some of the U.S. ports of entry, and one where the disruption was known about in advance and well anticipated. One can easily estimate that the impact would have been factors higher (if not exponentially higher) if all the ports were closed without notice. How much could the economy withstand before collapsing? At the firm level, a number of examples illustrate the magnitude of the risk of disruption to business operations and the ability to conduct trade.

The terrorist attacks on September 11, 2001, had dramatic and lasting effects on automotive manufacturers dependent on not quite just-in-time deliveries across the U.S.-Canadian border, shutting down five Ford Motor Company plants in the U.S., for example.<sup>6</sup>

A recent study<sup>7</sup> of 861 firms over a nine-year period of time illustrates the significant impact of supply chain glitches on firm valuation: Each glitch had a lasting impact on the stock valuation of publicly traded firms, calculated to be a permanent loss of approximately 9 percent of the stock valuation after announcement of the glitch. “This translates into

an average destruction in shareholder value in 1998 dollars of about US\$130 million per glitch. For the 861 glitches in the sample, this amounts to an overall destruction in shareholder value of about US\$112 billion.”<sup>8</sup>

A now-famous lightning bolt at a radio frequency chip plant in New Mexico virtually started a chain of events that resulted in Ericsson’s eventual departure from the cellular phone production business.<sup>9</sup> The case presents a unique side-by-side comparison of how two firms (Ericsson and Nokia) were able to respond to a situation and how the preparedness, systems, and organizational capabilities were the differentiating factors in their starkly different performance. While a number of factors contributed to the demise of Ericsson’s cellular phone business, their lack of a sensing, aware, and responsive organization—and Nokia’s highly sensing, communicative, and aware organization—determined the outcome of the disruption, with the viability of the firm clearly at stake.

A growing number of examples could be used to make the point—secure supply chains enable firms to continue exchanging goods and services, creating a healthy economy. Without the ability to source, produce, and distribute product to customer demand, there would be no economy.

## Options to Create Additional Collateral Benefits

Firms have a variety of investment options available to improve their supply chain security. The box below provides an overview of a range of security investments offering collateral benefits, and Table A.1 in the Appendix provides a more complete version,

also showing the direct and collateral benefits associated with these investments. The Appendix is designed to portray a range of security investment options and the associated broad range of anticipated collateral benefits. It is notable that a firm may create similar collateral benefits by making different supply chain security investments. Therefore, the table provides guidelines for understanding the potential collateral benefits available prior to making an investment decision, to maximize the potential collateral benefits and the subsequent return on investment. Each entry in the table will be addressed in subsequent sections.

## Collateral Benefits from Asset Visibility and Tracking

Firms can make a number of investments that provide varying levels of asset visibility and tracking. Asset visibility provides constant access to location and product status, which may reduce the uncertainty of shipment arrival. Together with product tracking, asset visibility also provides a time-definite and controlled chain of custody for conveyances across the supply chain. They give firms higher levels of security by providing a more consistent and predictable flow of materials, making it easier to observe exceptions to anticipated material flows that may indicate a security breach and allowing subsequent rapid follow-up and preventative actions.

Within this category of security investment, firms have many choices, each with a different potential for creating collateral benefits. Global Positioning Systems (GPS) are widely used now for tracking the location of truck and rail fleets. Radio Frequency Identification (RFID) and Smart Containers are in the early stages of being developed for commercially viable applications for asset tracking.

### An Overview of Supply Chain Security Investment Options Offering Collateral Benefits

- Asset Visibility and Tracking
- Personnel Security
- Physical Security
- Standards Development
- Supplier Selection and Investment
- Transportation and Conveyance Security
- Building Organizational Infrastructure Awareness and Capabilities
- Collaboration Among Supply Chain Parties
- Proactive Technology Investments
- TQM Investments
- Voluntary Security Compliance

The collateral benefits may be significant with this set of investments, although they will not be automatic. By providing constant access to location and product status, planners may be able to reduce the specified inventory levels because they have less uncertainty in the material flows. Lower inventory levels and less uncertainty may result in lower operating expenses coming from less product handling and rehandling, which is common in distribution systems with high levels of uncertainty. Achieving these collateral benefits, however, will require the firm to actually reduce the inventory levels, potentially reduce the planned transit times, and even modify transportation arrangements with third parties to take advantage of the lower levels of uncertainty and potentially even fewer shipments (emergency shipments especially).

### **Collateral Benefits from Personnel Security**

By focusing on the “supply” of human resources, firms can increase the level of security within the firm. The focus on people is one of the most fundamentally important aspects of supply chain security. This may entail a thorough initial background check to eliminate “bad actors” from the hiring pool, supplemented with regular drug testing and background checks. These will increase the likelihood of providing early warning about employees operating under the influence, or early warning about those employees with intent on putting the firm and its assets at risk. The testing does come at a cost, but it has been long recognized that one of the most significant risk elements is “the enemy within” the walls of the corporation.

In an odd twist, it is likely that employees will place a higher value on their employment with the recognition that the firm establishes and maintains a high quality level for employees, building pride in their work and greater dedication to the firm’s objectives.

Just as employees may value the high standards, so too will the customers appreciate the high personnel and operating standards. Increased customer loyalty, increased sales revenues, and higher market shares are possible from the higher levels of employee commitment coming from the firm’s efforts to maintain high employee standards.

### **Collateral Benefits from Physical Security**

Physical security is commonly one of the first security initiatives that firms undertake to improve system security. Physically preventing access and controlling access keeps out unauthorized personnel, protecting site intellectual property, capital equipment, personnel, inventory, work in progress, finished goods, and product integrity. Traditional approaches to security have focused on theft reduction, which entails protecting against the unauthorized removal of items from the process. Physical security investments often focus on local site security and not system-wide security. The new security paradigm, however, now requires inverse thinking by developing systems that prevent the addition of unauthorized items into the supply process.

These investments may provide other benefits as well, including increasing process efficiency through technology adoption (e.g., automated processing and identification through technologies like radio frequency identification), and reducing Overages, Shortages, and Damages (OS&D) from potentially fewer handoffs and more automated handling. These lower loss levels may generate their own collateral benefits. With lower loss levels, insurance rates will likely drop because of the reduced likelihood of loss, and firms can expect lower indirect costs (short-term administration costs and long-term expenses) that are not reimbursed by typical insurance policies.<sup>10</sup>

For firms regularly hosting customers on site, a more secure environment certainly provides for a much more favorable experience and builds confidence in the supplier selection, increasing the likelihood of continued business and return visits by customers.

### **Collateral Benefits from Standards Development**

Firms often invest resources in building industry operating coordination and security standards. These pay many direct benefits, making it easier to coordinate multi-company security activities (initiatives, stinging operations, incident investigations), making

security breaches easier to spot, making for higher levels of security, and ultimately improving the security of the entire system, not just the individual firm. Standards may help reduce non-security losses through processes that entail systems-wide awareness and incentives and practices oriented toward security. The benefits surface in non-security loss reduction such as reduced counterfeit and “gray market” shipments. As one global logistics security manager said, “We’re structured as a group within [the firm] to try and delve into more of those business issues that are out there—counterfeit, gray market, supply chain, warranty fraud, etc., where

through some of our efforts we’ve been able to show a return to the bottom line....”

Beyond these direct benefits, developing standards may also generate potential collateral benefits. By having standards for security, coordination, and operation, firms may find improved efficiency in various logistics operations, potentially resulting in reduced shipping times. Industry standards often lead to higher levels of process discipline that are necessary for intercompany operations, leading to higher performance levels from fewer process deviations and increased process predictability.

Security Investment	Direct Benefits	Collateral Benefits
Asset Visibility and Tracking	<ul style="list-style-type: none"> <li>• Provide positive location status, preventing excursions</li> <li>• Provide time-definite and controlled chain of custody</li> </ul>	<ul style="list-style-type: none"> <li>• Lower theft and losses</li> <li>• Faster recalls</li> <li>• Fewer delayed shipments</li> <li>• Better planning, enabling lower working capital for inventory</li> <li>• Less Overages, Shortages, and Damages (OS&amp;D)</li> <li>• Protection of brand name</li> </ul>
Personnel Security	<ul style="list-style-type: none"> <li>• Thorough background check eliminates “bad actors” from hiring pool</li> <li>• Regular background checks provide early warning for employees operating under the influence</li> </ul>	<ul style="list-style-type: none"> <li>• Customer loyalty, increased sales revenues, higher market share</li> <li>• Employee commitment and belief in company’s concern for employee</li> </ul>
Physical Security	<ul style="list-style-type: none"> <li>• Controlled access keeps out unauthorized personnel</li> <li>• Protection of intellectual property</li> <li>• Protection of capital equipment and personnel</li> <li>• Protection of product integrity</li> </ul>	<ul style="list-style-type: none"> <li>• Customer recognition of firm’s safe and secure environment as an expertise, increasing customer loyalty</li> <li>• Fewer thefts and OS&amp;D by virtue of having more secure facility</li> <li>• Reduced equipment damage and operating costs (lower insurance rates)</li> <li>• Fewer safety incidents and catastrophes</li> </ul>
Standards Development	<ul style="list-style-type: none"> <li>• Facilitate coordination of multi-company security activities (initiatives, sting operations, incident investigations)</li> <li>• Security breaches easier to spot with standard systems</li> <li>• Higher levels of security with common procedures</li> <li>• System-level and supplier security improvement</li> </ul>	<ul style="list-style-type: none"> <li>• Improve the efficiency of ship, train, truck, terminal operations; cuts international shipping times</li> <li>• Platform for collaboration within an industry leading to standards that raise level of performance</li> <li>• Process discipline enables compliance (quality, safety, process), higher performance</li> <li>• Common processes reduce confusion, raise predictability, improve staff backup</li> <li>• Reduce non-security losses</li> </ul>

## Collateral Benefits from Supplier Selection and Investment

Investing in secure suppliers is a fundamental source of supply chain security. It is difficult to overstate the importance of the security of the firm's suppliers, and suppliers throughout the supply chain, including those upstream from the tier-one supplier. This comes as a result of the increasing interdependencies among supply chain parties, particularly as firms outsource more activities to third parties, inherently bringing in greater risk of security breach. End-to-end supply chain security is therefore of fundamental importance to overall supply chain security.

Basic expectation sharing, supplier site visits, and security audits increase the likelihood of higher levels of security in the upstream supply chain. Additionally, firms may elect to more deeply involve selected suppliers in tabletop and mock incident exercises, further increasing the upstream supply chain security. Some firms consider this a mandatory set of actions required to validate the supplier's ability to maintain a secure supply. While a firm may wish to trust a supplier's intent, the necessity is to check the supplier's capabilities. Aside from ensuring the integrity and uninterrupted supply of materials, such discipline also provides the firm with a direct insight into the supplier's ability to maintain a supply in a potential security breach or disruption.

Focusing on supplier security also indoctrinates the supplier to sense security issues, providing an early warning system for the firm, on security issues as well as other critical issues such as quality and availability. Ultimately, these efforts result in lower levels of loss, less downtime, and likely higher quality. By collaborating, sharing resources, and working toward common goals, firms may be able to enjoy lower costs from reduced cargo inspections, faster throughput, joint planning, ongoing coordination, and active problem resolution. Firms that develop and maintain a clear "secure supplier" competence maintain a marketing advantage for customers that demand security in their own supply chains.

## Collateral Benefits from Transportation and Conveyance Security

Investing in securing transportation conveyances may provide significant security benefits. The options include adding additional drivers to avoid long stops ("freight at rest is freight at risk"), adding physical security features to the conveyance (e.g., electronic seals), and adding visibility tools to maintain known location and status (e.g., GPS and RFID systems). These will likely result in lower losses from theft, fewer incidents of product adulteration, lower OS&D, avoidance of cargo misuse (e.g., as a weapon delivery system), and protection of the conveyance itself.

A distinct collateral benefit exists for the supplier in cases where the supplier develops a secure operation and leverages this as a competitive advantage. In several instances, firms have used their security practices and orientation as a competitive advantage in capturing additional business in the marketplace.

## Collateral Benefits from Building Organizational Infrastructure Awareness and Capabilities

Making investments in organizational infrastructure constitutes a long-term approach toward building capabilities in the organization through personnel and organizational processes. Typical efforts might include investing in employee education on vulnerability and on firm operations, building improved communications systems, and adding security measures into performance assessment and incentives, among others.

How do these investments impact security and provide collateral benefits? As an example, regular communication about security issues that is woven into daily work practices builds an awareness of security issues that translates into quicker recognition of security breaches and issues when they arise. Similarly, this establishes a knowledge base in every employee that is broad, with each employee being well informed and aware of the broader system and its operation. This, in turn, develops employees that are more aware of the firm's broader business needs and issues, and hence those employees can con-

Security Investment	Direct Benefits	Collateral Benefits
Supplier Selection and Investment	<ul style="list-style-type: none"> <li>• Ensure a secure supply of materials</li> <li>• Early warning of upstream security issues</li> <li>• Reduce upstream and inbound losses</li> </ul>	<ul style="list-style-type: none"> <li>• Lower inspection costs, faster throughput</li> <li>• Enhanced communication via collaboration</li> <li>• Increase efficiency through joint planning</li> <li>• Utilize internal security resources to assist suppliers, ultimately making for improved relationships</li> </ul>
Transportation and Conveyance Security	<ul style="list-style-type: none"> <li>• Reduce theft losses</li> <li>• Reduce adulteration of product</li> <li>• Reduce chance of cargo vessel misuse (weapon delivery system)</li> <li>• Protect conveyance equipment, vessels</li> </ul>	<ul style="list-style-type: none"> <li>• Cost avoidance of non-product-related costs (indirect costs)</li> <li>• Crime and vandalism rates fall</li> <li>• Fewer disruptions to the supply chain, more cost savings compared with avoided losses</li> <li>• Less capital required for inventory</li> <li>• Reduced transportation cycle time</li> </ul>
Building Organizational Infrastructure Awareness and Capabilities	<ul style="list-style-type: none"> <li>• Build awareness of security concerns</li> <li>• Increase role of security in daily operations and every assignment</li> </ul>	<ul style="list-style-type: none"> <li>• Increase problem prevention through recognition by employees</li> <li>• Increase early intervention, reducing impact of a disruption</li> <li>• Improve the ability to respond with early awareness</li> </ul>
Collaboration Among Supply Chain Parties	<ul style="list-style-type: none"> <li>• Improved coordination along supply chain increases security</li> </ul>	<ul style="list-style-type: none"> <li>• Platform for broader alignment</li> <li>• Enable creation of a secure supply chain network for common problem solving, resource sharing</li> <li>• Improve communication among supply chain partners, potentially reducing coordination costs</li> </ul>

sider them when making operating decisions. The likely results are decisions that are more closely aligned with the business needs.

Specifically, organizational infrastructure investments may then increase problem prevention through problem recognition by employees. In addition, such investments may increase the chances that employees may recognize potential problems, which enables the firm to intervene and reduce the impact and consequences of a disruption.

One firm described how their infrastructure investments helped build an exceptionally resilient and responsive supply chain. Each day employees receive a three- to four-minute security brief that is integrated into a daily communications meeting at the beginning of each shift. Since all critical issues in the business are covered together, security is recognized on a par with the other key elements of the business operation. Employee performance measures include losses as a key element, and incentives and rewards are offered to employees for specific actions taken to reduce losses.<sup>11</sup>

## Collateral Benefits from Collaboration Among Supply Chain Parties

Similar to making investments in organizational infrastructure, investments in collaboration entail a long-term approach toward building capabilities in the supply network through inter-organizational processes. Typical efforts might include investing in building formal communication systems, facilitating regular interactions between multiple levels within each organization,<sup>12</sup> and conducting joint security assessment and response planning. As noted previously, the collaboration among supply chain parties may include multiple partners together in tabletop and mock incident exercises. Such proactive work further increases the awareness and likelihood of increasing end-to-end supply chain security.

Collaboration in the supply chain can also be security specific. In some cases, firms may elect to build security into their extended supply network by using third parties for security contracting. In other cases, firms may elect to develop long-term contracts or, perhaps more importantly, mutually agreed terms

and conditions among the supply chain parties so that the organizations can operate more efficiently and effectively. These investments may also foster the development of closer relationships and more easily align the parties around the shared objective. This may result in higher performance levels, as well as higher levels of awareness as each organization develops a deeper understanding of the other's operating characteristics and needs.

## Collateral Benefits from Proactive Technology Investments

Investments in technology are often praised for generating numerous benefits beyond the initial purpose of the investment. Investing in technology for security is no different, where the investments create the ability to customize the application to the benefit of the firm and potentially provide visibility throughout the supply network. Visibility investments enable increased real-time awareness of business operations and better process knowledge, which in turn enables the firm to focus resources and efforts on key improvement areas, therefore reducing waste and increasing resource utilization.

Two examples illustrate these benefits. In the first case, one firm<sup>13</sup> elected to install a new security technology before the government-mandated adoption of the technology. Although this required an initial outlay for the technology, the firm believes this will ultimately result in lower costs since they were able to design the system around their own processes and systems. Specifically, the firm built other processing systems into the technology that avoided adding another step in their process, streamlining the operations and therefore reducing their cycle time and operating costs. Had the company waited, it is unlikely that the government would have been so open to designing other features into the system, so the firm would have been forced to adopt a system that did not “fit” with their operating system.

The second example illustrates how one firm in the medical supply industry used an early warning information systems to provide data about specific customer needs during a disruption. Their analysis indicated that the firm actually had 48 hours to respond to a disruption before it impacted the customer, allowing the firm to plan for less expensive

two-day service rather than the more costly next-day service in responding to the disruption.<sup>14</sup>

In both cases, firms proactively invested in technology and systems intended to improve security and at the same time enabling the firms to create additional benefits of great value.

## Collateral Benefits from TQM Investments

The underpinnings of the “total quality management” (TQM) approach to security improvements have potential collateral benefits in a number of significant areas. The hallmarks of TQM are dedication of the entire organization and its suppliers (and in some cases its customers) to improved security, emphasis on prevention of security breaches, assurance that the security system is operating “in control” within a defined set of parameters, and the embedding of security in the firm's business processes.

Operating “in control” when using a TQM approach to embed and document security in the logistics processes can lead to a reduction in safety stock, lead-time variance, and reduced OS&D shipments.<sup>15</sup> Because the process is operating within defined limits and with emphasis on internal discipline, shipments should be more accurate and can be counted on with greater reliability to precisely meet shipping specifications. Information provided to logistics managers within the firm should also be counted on to provide accurate representations of the goods that are in transit. These same capabilities provide useful benefits to non-security areas, such as reduced variation in operations, which results in lower operating costs, and higher levels of employee awareness. And better decisions, likely higher resource utilization, and higher levels of service may be possible through process improvements that aware and enlightened employees may initiate and implement.

Other capabilities and potential for improvement can be derived by using the enhanced information gained from the TQM process. This rigorously collected data may offer greater visibility within the supply chain, enabling improved materials tracking and early problem identification by discerning bottlenecks and congestion.

## Collateral Benefits from Voluntary Security Compliance

While the U.S. moved ahead first with initiatives to upgrade trade and transportation security, other countries as well have passed new legislation or undertaken new initiatives. Most of the initiatives involve approaches similar to those undertaken in the U.S. They are based primarily on voluntary efforts by companies to improve supply chain security and include a benefit in terms of facilitated customs processing for participating companies. Canada's Partners in Protection, Sweden's StairSec, and the European

Union's Authorized Economic Operator program contain the central themes of voluntary actions to improve supply chain security and a benefit of facilitated customs processing in exchange for the security improvements. The World Customs Organization is moving toward an international framework for supply chain security and customs processing. It adopted the Resolution on Global Security and Facilitation Measures Concerning the International Trade Supply Chain, which aims to create an international system for identifying businesses that offer a high degree of security in their supply chain operations and to provide customs facilitation for those companies.

Security Investment	Direct Benefits	Collateral Benefits
Proactive Technology Investments	<ul style="list-style-type: none"> <li>• Technology provides increased ability to track, monitor, and observe material flows, preventing excursions</li> </ul>	<ul style="list-style-type: none"> <li>• Ability to customize the application to the benefit of the firm</li> <li>• Increase process efficiency through technology</li> <li>• Visibility investments give real-time awareness of supply chain delays, location, and status</li> </ul>
TQM Investments	<ul style="list-style-type: none"> <li>• More consistent security procedure execution</li> <li>• Application of Six Sigma may lead to disciplined loss reduction efforts</li> <li>• Lower losses</li> <li>• Higher-performance employees emphasize security</li> <li>• Process design standardizes security processes</li> <li>• Design supply chain with fewer handoffs, keeping product moving</li> </ul>	<ul style="list-style-type: none"> <li>• Discipline increases, enabling compliance (quality, safety, process)</li> <li>• Reduction in safety stock, lead-time variance, and lower OS&amp;D</li> <li>• Better process knowledge and management from additional data, greater visibility to discern bottlenecks and congestion</li> <li>• Safety stock reduction as a result of advance lead-time information</li> <li>• Investment in quality processes results in quality security</li> <li>• Consistent process operation leads to fewer disruptions, faster and more reliable operation</li> <li>• Process discipline leads to higher levels of performance, efficiency</li> </ul>
Voluntary Security Compliance	<ul style="list-style-type: none"> <li>• European Union's Authorized Economic Operator program ensures base level of supply chain security assessment</li> <li>• Customs specialists working in specialized security programs may observe risk of security breach before breach can occur</li> <li>• Customs-Trade Partnership Against Terrorism (C-TPAT) membership provides member companies with information about industry "best practices" in supply chain security</li> <li>• Sweden's StairSec program leads to higher inspection rates of uncertified cargo, increasing likelihood of early warning and prevention</li> </ul>	<ul style="list-style-type: none"> <li>• Establish a "mandatory" fundamental standard across industry for supply chain security via a "voluntary" program</li> <li>• A platform for collaboration and alignment within an industry that leads to industry standards, raising overall level of performance in quality, service, and cost</li> <li>• C-TPAT supply chain specialist assists firm as CBP liaison for validation, security issues, procedural updates, communication, and training</li> <li>• Faster border throughput times from fewer inspections and "green lane" flow, which may raise service levels, enabling lower working capital</li> <li>• Process discipline enables compliance (quality, safety, process), higher levels of process performance</li> </ul>

While it is officially a voluntary security program, the U.S. Customs-Trade Partnership Against Terrorism (C-TPAT) program for all intents and purposes is nearly a “mandatory” program.<sup>16</sup> The disadvantages for those firms that do not volunteer are significant—e.g., higher rates of inspection that may add extra time of up to 10 to 12 days in a congested U.S. seaport and uncertainty in customs processing. For those firms that elect to participate in C-TPAT, there is a clear program compliance requirement. Regardless of the firm’s intent in participating in C-TPAT, one collateral benefit of this implicit regulation is that C-TPAT effectively serves as the foundation process for implementing supply chain security for many firms, which is a significant benefit.

Recent results from those firms participating in C-TPAT report that there are indeed tangible benefits available. U.S. Customs and Border Protection (CBP) reports that firms participating in C-TPAT have received tangible benefits in terms of reduced customs examinations. They report that “in the Automated Commercial System (ACS), C-TPAT certified importers received reduced selection rate for compliance measurement examination (-3x in FY 2003) and exclusion from certain trade-related local and national criteria,” and that C-TPAT certified importers receive targeting benefits (-7x in FY 2003) by receiving a “credit” via the CBP targeting system.<sup>17</sup>

### **Faster Flow Through Customs**

Participating in the various government/industry programs that are becoming more prevalent throughout the world provides access to a “green lane” for imports, which would entail expedited customs clearance, effectively speeding material flows through the import supply chain process.<sup>18</sup> Faster throughput times at border crossings also come from fewer inspections by virtue of being in compliance with government regulations. The faster throughput may raise service levels and lead to other benefits, not the least of which include faster delivery to customers, lower working capital for inventory, and lower operating costs from less handling and fewer movements.

For some firms, this is the most important collateral benefit: “The overarching elements that define the [company] have to do with speed and flexibility. The second [that not being C-TPAT certified] was viewed

as an impediment to speed, it became a high priority. If this thing didn’t intersect with speed and flexibility, it would be a ‘who cares?’ But because it could conceivably play havoc with speed and flexibility, it became a high priority. The fact that it was a potential impediment was quickly obvious internally.”<sup>19</sup> Another firm placed a conservative cost-savings figure on their C-TPAT compliance, saying that it will save \$12 million in cost by reducing the actual cost of the inspection.<sup>20</sup> This figure did not include any other likely benefits such as capital/inventory, coordination, or service-related cost reductions, meaning that a more realistic assessment would put the actual financial impact for the firm at multiples of their estimate.

### **Potentially Faster Restart and Flow Through Customs Post Disruption**

A widely anticipated but not yet promised or defined benefit of participating in government security programs is favorable treatment after future disruptions. Although customs officials have made no commitments to provide this benefit, it seems logical that they will select “known shippers” and other firms participating in government programs among the first cargo to be permitted through customs after a disruption.

### **Platform for Collaboration**

These programs provide a platform for collaboration and alignment within an industry that leads to industry standards, raising overall level of performance in industry on several levels, not just security. Specifically, these programs provide a network of firms that enables higher levels of coordination for tackling common industry problems. At one firm, the “collateral benefit of [the] security program has been open communication with competitors such as Wal-Mart. It’s the industry’s best interest to share information to help protect.”<sup>21</sup>

### **Supply Chain Efficiency**

A number of voluntary programs entail several common practices that may help to improve supply chain efficiency as they improve security. Practices such as early warning systems—for example, electronic prenotification of delays or problems in customs clearance—enable the affected parties to react quicker and with more reaction time. This ultimately makes for a more thoughtful response that will tend to be

more effective and will utilize resources better. As an example, one medical products producer noted that its early warning systems give it 12 to 24 hours to respond before problems impact customers, enabling them to use the precious time for optimal response planning and execution. As it turns out, this foreknowledge allowed the firm to reduce emergency transportation costs and more effectively allocate reserve inventory. With some forethought, firms will be able to anticipate efficiency and effectiveness improvements in their supply chain operations.

### **Broader Impact on the Firm**

Participating in voluntary programs also integrates security into standard processes, engraining security into the process fabric of the firm. This becomes an important element in creating a security culture that increases the level of awareness and sensitivity in the firm to potential security breaches and system disruptions.

Others have noted that C-TPAT partners have enjoyed additional collateral benefits, including lower theft and losses, as well as reduced insurance rates after firms adopt improved security procedures.<sup>22</sup>

Many of the programs serve to instill process discipline in the firm, which increases compliance and higher performance in other domains such as quality, safety, and process performance. As an example, The Gillette Company learned that multiple methods were being used in the firm to handle imports, making for inefficiencies and additional costs to handle the multiple methods.<sup>23</sup>

“While preparing its C-TPAT application, for example, The Gillette Company discovered that each of its subsidiaries had different ways of handling imports, said Global Customs Compliance Manager Norman Lubeck. He’s now working on standardizing import procedures company-wide, which will bring both cost and efficiency benefits.”<sup>24</sup>

# Achieving Collateral Benefits

## Connecting Security Investments and Collateral Benefits

Recognizing the potential to augment the return on supply chain security investments, firms may wish to actively pursue creating collateral benefits. Yet these benefits are not guaranteed because the investments themselves do not automatically create collateral benefits. Instead, the security investments create the opportunity—either through a new capability, a new process, or a different business condition—which could then be used to create a collateral benefit. To fully understand how to create the collateral benefit from the security investment, one must analyze and detail the causal relationship between the security investment and the actual benefit. This is a critical element when developing a realistic business case for the security investment.

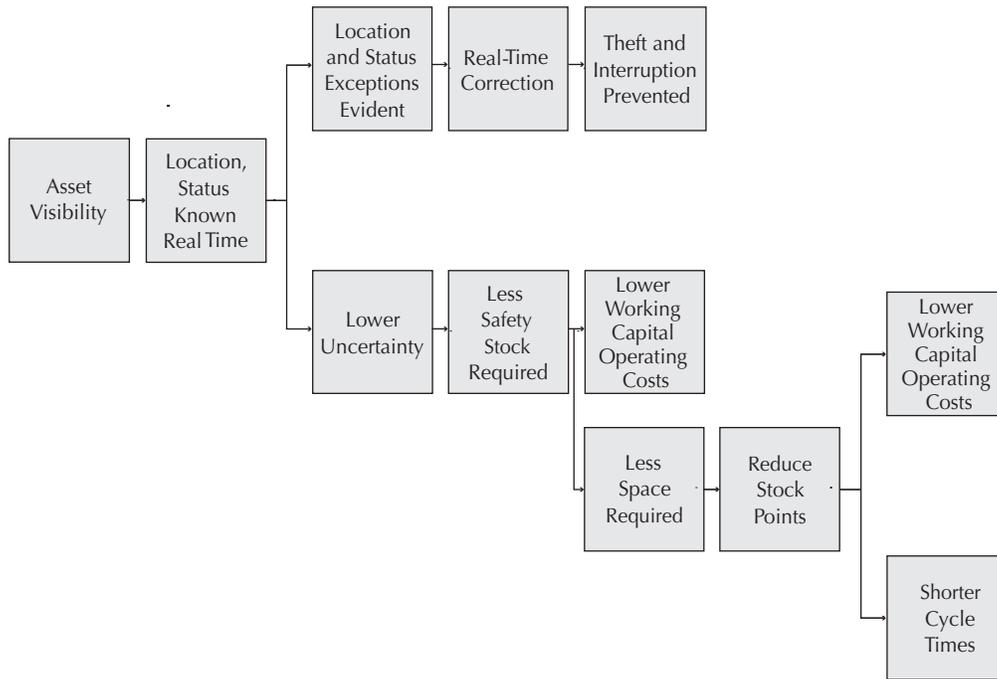
While we have suggested and even enumerated a broad range of collateral benefits that could potentially be derived from a variety of security investments, most of these possibilities are based on preliminary data<sup>25</sup> and early insights rather than formal data collection and analysis. The good news is that such speculation can be made with some foundation because one can find guidance from similar past investments. Many of the potential investments predictably create certain capabilities, some of which have known impacts on supply chains, enabling one to develop a linkage map from the investment to benefits. A linkage map may illustrate the relationship between a security investment and the subsequent capability that is created, which in turn enables subsequent action and potential benefit. An example may help illustrate the possibility.

## Making the Connection: Collateral Benefits Linkage Maps

For example, investing in tracking systems to provide asset visibility may provide a valuable security service/role, but it is also believed to reduce uncertainty in the supply chain with real-time confirmed asset location and status/condition. With such information, supply chain managers have less uncertainty and could therefore reduce the amount of safety stock necessary. If the manager does reduce the safety stock, this will reduce working capital and operating cost (lower levels of inventory to finance, fewer movements to make). With lower levels of inventory, the firm needs less space for that inventory, reducing the amount of stocking space required (eliminating interim stock points or reducing contracted space commitments). If the firm eliminates interim stock points, they will enjoy lower operating costs (fewer stock points and less handling from fewer movements) and potentially faster cycle times (fewer stops, less time handling/stocking/shipping).

This example, illustrated in Figure 1, shows the potential for creating collateral benefits by identifying the linkages between the investment and the benefit. Capturing and achieving the benefits, however, requires that the firm take action (in the example given, reducing inventory and eliminating stock points). Additionally, in some cases the collateral benefits can also be attributed to other conditions as well, so there may be other requirements that need to be present in order to capture the benefits.

**Figure 1: Example of a Collateral Benefits Linkage Map**



Again, this intends to show that these collateral benefits are possible. The order of magnitude is dependent on the scope and the success of the implementation, and clearly the firm would need to take action in order to enjoy the gains. As suggested earlier, the ability of the firm to enjoy the collateral benefits is also dependent on other conditions as well. This includes whether the firm actually takes action to reduce inventory levels, to use the additional information in its planning, and even to eliminate intermediaries. So we can assert that the investments can create possibilities, but enjoying the advantage requires other conditions as well; it's not automatic, and therefore creating and leveraging the collateral benefits will take management attention and action.

## Challenges and Choices for Creating Collateral Benefits

### Minimalist or Holistic Systems Approach?

An initial observation from interviews with security leaders indicates that firms are taking one of three approaches to implement supply chain security:

doing nothing, making minimal efforts targeted at satisfying voluntary program compliance obligations, or making holistic efforts targeted at improving the overall system.

The “do nothing” group has chosen to make no investment in supply chain security. These firms appear to be fatalists and presume that a terrorist attack or disruption will affect all companies equally. Based on that, they have chosen to take no action at all and will not receive the benefits associated with security investments.

Slightly more involved are those firms that take a “minimalist” approach. Here, the firms undertake the bare minimum required to satisfy participation requirements for voluntary government programs. As an example, one high-tech company selling consumer products stated that their supply chain security approach depends completely on complying with a government security program: “We’re pursuing C-TPAT certification, and that’s our security plan.”<sup>26</sup> In these cases, the firms will likely enjoy lower security operating costs and may receive limited collateral benefits from their security invest-

ments, but may be vulnerable to security breach or other disruptions and may also suffer higher losses and delays in their respective supply chains.

In comparison to these two groups, firms adopting a holistic approach undertake a comprehensive effort to impact the entire system (i.e., the end-to-end supply chain) rather than just meeting voluntary program compliance obligations. This group is most likely to realize collateral benefits from their security investments. One firm pursuing a holistic systems approach invested significant sums above and beyond that which was needed for C-TPAT compliance to improve the security of their supply chain, and the firm enjoyed several benefits. In addition to eliminating losses on new product introductions, the firm enjoyed the collateral benefits of new levels of collaboration in their industry, and their C-TPAT application required no additional efforts to gain compliance. Ultimately, this firm, in adopting the more holistic approach, has created a more secure supply chain, with lower loss levels, and improved their overall end-to-end supply chain efficiency and performance, with these benefits far exceeding the investment costs.

### **Making Investment Choices**

Firms have supply chain security investment choices, and the best option for one firm may not be the best option for another firm. The specific benefits, costs, risks, and requirements need to be assessed by the firm in order to make a determination as to what is best for the firm itself.

Prior to making investment decisions, it may be possible and useful to consider several characteristics of the various security investments that can possibly create collateral benefits:

- Effort required to implement the security initiative
- Collaboration required to achieve the collateral benefits
- Cost of implementing and additional efforts required to create the collateral benefits
- Estimated time for collateral benefits, i.e., whether the collateral benefit could be enjoyed in the near term or long term

These may provide a starting point for firms to consider the possibilities.

# Conclusion

## Observations and Issues to Consider

While this report has introduced several new concepts and proposed some new management and policy actions, a number of other directly relevant and tangential issues are worthy of some discussion. Some of these are offered here, as it may be useful for organizations to consider these preliminary observations when planning their investment decisions.

Most notably, the preliminary analysis shows that the major collateral benefits accrue from reducing actual security breaches and enabling trade continuity or “trade security.” Some firms place the value of this as high as US\$50–100 million/day cost, and in one actual case, one firm’s “trade security” enabled it to avoid the US\$250 million loss that its less secure competitor suffered.

It also appears that there is some “first mover advantage” possible to firms if they engage early enough in the process. One firm described how it was able to establish an important security standard by volunteering to install security equipment as a beta site for the local government, therefore building the standard around its own internal processes, which subsequently made for a faster throughput and lower operating cost for the firm.

Some forward-thinking security efforts have engaged the corporate accounting or finance operations, in one case installing a security chief who also was a CPA. Their experience indicated that this officer enjoyed increased success of making security investments and creating collateral benefits by virtue of knowing how to quantify benefits and credibly articulate this into the management hierarchy.

A significant collateral benefit may come when the firm ties the role of security to corporate objectives (i.e., security plays an integral role in the delivery of the product or service to the customer) rather than treating it merely as a separate activity. One firm in the fashion industry found it less expensive to spend US\$500,000 on security by hiring personnel to be on site (this added about US\$.01 per US\$200 item); the on-site resource established a robust security program, making their upstream supply chain more secure and thoroughly preparing them for the subsequent C-TPAT application. For this fashion product provider, time to market was critical, and so a key motivation for making the security investment was the speed advantage offered by being C-TPAT certified.

Finally, the importance and impact of voluntary programs is likely to increase as customs clearance processes require greater oversight and time. It is widely recognized that there is a capacity constraint in moving materials through many ports throughout the world. And with processes requiring more oversight, one can predict that there will be increasing delays for border crossings—delays that entail an implicit cost (cost of delay, cost of additional inspection) and will increase. Hence, the value of having security certification under a voluntary government/industry program will likely increase.

## The Challenge and Opportunity

This report presents an informed point of view on collateral benefits available to those making security investments. The work is based on insight, experience, secondary data, and anecdotal primary data, providing a qualitative assessment that portrays

the landscape relevant to developing and capturing collateral benefits from supply chain security investments. Far from being a foregone conclusion, though, capturing collateral benefits will require the important next step of validating these observations and further documenting the actual dynamics associated with identifying and achieving collateral benefits from supply chain security investments.

Creating and achieving collateral benefits requires a number of other capabilities and conditions in order to capture the benefits. Often, the collateral benefit enables a capability that must then be further developed and applied. Even for those instances where there is a direct causal relationship between a security investment and a capability, firms still need to take the initiative to exploit the potential. Interestingly, the potential will vary somewhat by firm, depending on firm characteristics and competitive situation, among other factors.

From the perspective of the firms that are considering supply chain security investments, the good news is that this preliminary analysis indicates there are many potential collateral benefits that may be derived from the investments. The lack of documented evidence to make the case should not be interpreted as an indication that attaining the benefits is impossible; this is more likely a result of the relatively recent recognition of security weaknesses and this emerging opportunity. One should not be surprised that there is a lack of systems to measure the impact of the security investment, much less the impact of collateral benefits. The management information systems need to be refined, and the organizational focus needs to be sensitized to observe and measure this data.

Those firms choosing to take a deeper look at the potential of creating the various collateral benefits will need to honestly and realistically assess the effort level and likelihood of success of their efforts to create collateral benefits. By virtue of undertaking this effort, firms will enjoy the collateral benefit of a more intimate understanding of their own operations, processes, capabilities, and weaknesses. This enables the firm to take even greater advantage of the possibility by tailoring the efforts to their firm-specific situation.

If this were easy, of course, all firms would be undertaking these activities, and copious amounts of data would be available to guide the uninitiated. Yet, the fact that achieving collateral benefits remains a challenge may have a positive twist to it—it clearly indicates the potential to create some competitive advantage for firms successfully seizing the opportunity and capturing these potentially significant benefits. A key turning point will occur when the early adopters promote their successes, demonstrating the potential economic value and competitive advantage from their investments in supply chain security.

## Looking Ahead

The international trade and transportation system remains vulnerable to an attack by terrorists who seek to strike at the heart of the underpinnings of modern economies. It is widely understood by government leaders and business executives that protection of the systems of trade and transportation are the exclusive province of neither the government nor the private sector. Neither has the means to completely supervise the vast number of activities that constitute international trade. Governments and firms working together, each operating within their realm of effectiveness, can, however, greatly reduce the opportunities for attacks by terrorists against the system of international trade.

The creation of collateral benefits from investments in security may very well be the fulcrum that balances the government's interest in increased security with the private sector's interest in increased efficiency. Without collateral benefits, increases in security will be viewed only as increases in costs. The natural reaction of the vast majority of firms when faced with a requirement that increases their costs will be to act entirely rationally. They will devise a strategy to reduce the costs and drive them to the lowest possible level. Governments that undertake a purely regulatory approach will find that many of the transactions that need to be controlled are beyond their reach, and that they have created a regulatory environment of increased costs and very uncertain benefits. The collateral benefits approach, however, allows governments to extend their reach deeply into the systems of international trade and allows firms to respond to the need for increased security throughout the trade process

in a way that enhances their competitive position. Collateral benefits work in consonance with free trade by allowing governments to attain a higher security content of international trade without regulating the details of the components of the transaction.

At this time, the collateral benefits approach contains a great deal of potential but remains difficult to quantify. There is little if any analysis of hard data documenting the actual collateral return on investments in security, as very few firms have taken a systematic and disciplined approach to understanding and creating collateral benefits. Firms need to be aware of the risks they take if investments are made in security with the hope that collateral benefits will flow from the investments but without the detailed planning and attention to managing change that are necessary to achieve the benefits. Just as was the case with many firms that pursued TQM without fully understanding the requirements, there are significant planning and change management obligations that are prerequisites to successfully creating collateral benefits.

Government regulatory agencies as well need to think outside their regulatory focus and understand how their decisions impact the operational realm of international trade. The “green lane” is a term used by customs organizations to describe how the customs formalities of firms certified to be secure will be processed. A green lane is meaningless, however, if it is an expression of customs processing that is not integrated with the actual operations of the port. At a seaport, chassis need to be available and dedicated lanes and special processing need to be available to expedite egress from the port. Government agencies need to pay close attention to the detailed planning and change management that are the foundations of collateral benefits.

Collateral benefits are an important component of the “new normalcy” of international trade—the quest to have it both ways, increasing both security and efficiency. A great deal of work remains to be done to convert the opportunity into actuality, with potentially significant benefits and competitive advantages available to those supply chains that are successful.

# Appendix: Overview of Supply Chain Security Investment Options

**Table A.1: Overview of Supply Chain Security Investment Options—Direct and Collateral Benefits**

Security Investment	Direct Benefits	Collateral Benefits
Asset Visibility and Tracking	<ul style="list-style-type: none"> <li>• Provide positive location status, preventing excursions</li> <li>• Provide time-definite and controlled chain of custody</li> </ul>	<ul style="list-style-type: none"> <li>• Lower theft and losses</li> <li>• Faster recalls</li> <li>• Fewer delayed shipments</li> <li>• Better planning, enabling lower working capital for inventory</li> <li>• Less Overages, Shortages, and Damages (OS&amp;D)</li> <li>• Protection of brand name</li> </ul>
Personnel Security	<ul style="list-style-type: none"> <li>• Thorough background check eliminates “bad actors” from hiring pool</li> <li>• Regular background checks provide early warning for employees operating under the influence</li> </ul>	<ul style="list-style-type: none"> <li>• Customer loyalty, increased sales revenues, higher market share</li> <li>• Employee commitment and belief in company’s concern for employee</li> </ul>
Physical Security	<ul style="list-style-type: none"> <li>• Controlled access keeps out unauthorized personnel</li> <li>• Protection of intellectual property</li> <li>• Protection of capital equipment and personnel</li> <li>• Protection of product integrity</li> </ul>	<ul style="list-style-type: none"> <li>• Customer recognition of firm’s safe and secure environment as an expertise, increasing customer loyalty</li> <li>• Fewer thefts and OS&amp;D by virtue of having more secure facility</li> <li>• Reduced equipment damage and operating costs (lower insurance rates)</li> <li>• Fewer safety incidents and catastrophes</li> </ul>
Standards Development	<ul style="list-style-type: none"> <li>• Facilitate coordination of multi-company security activities (initiatives, sting operations, incident investigations)</li> <li>• Security breaches easier to spot with standard systems</li> <li>• Higher levels of security with common procedures</li> <li>• System-level and supplier security improvement</li> </ul>	<ul style="list-style-type: none"> <li>• Improve the efficiency of ship, train, truck, terminal operations; cuts international shipping times</li> <li>• Platform for collaboration within an industry leading to standards that raise level of performance</li> <li>• Process discipline enables compliance (quality, safety, process), higher performance</li> <li>• Common processes reduce confusion, raise predictability, improve staff backup</li> <li>• Reduce non-security losses</li> </ul>
Supplier Selection and Investment	<ul style="list-style-type: none"> <li>• Ensure a secure supply of materials</li> <li>• Early warning of upstream security issues</li> <li>• Reduce upstream and inbound losses</li> </ul>	<ul style="list-style-type: none"> <li>• Lower inspection costs, faster throughput</li> <li>• Enhanced communication via collaboration</li> <li>• Increase efficiency through joint planning</li> <li>• Utilize internal security resources to assist suppliers, ultimately making for improved relationships</li> </ul>

Security Investment	Direct Benefits	Collateral Benefits
Transportation and Conveyance Security	<ul style="list-style-type: none"> <li>• Reduce theft losses</li> <li>• Reduce adulteration of product</li> <li>• Reduce chance of cargo vessel misuse (weapon delivery system)</li> <li>• Protect conveyance equipment, vessels</li> </ul>	<ul style="list-style-type: none"> <li>• Cost avoidance of non-product-related costs (indirect costs)</li> <li>• Crime and vandalism rates fall</li> <li>• Fewer disruptions to the supply chain, more cost savings compared with avoided losses</li> <li>• Less capital required for inventory</li> <li>• Reduced transportation cycle time</li> </ul>
Building Organizational Infrastructure Awareness and Capabilities	<ul style="list-style-type: none"> <li>• Build awareness of security concerns</li> <li>• Increase role of security in daily operations and every assignment</li> </ul>	<ul style="list-style-type: none"> <li>• Increase problem prevention through recognition by employees</li> <li>• Increase early intervention, reducing impact of a disruption</li> <li>• Improve the ability to respond with early awareness</li> </ul>
Collaboration Among Supply Chain Parties	<ul style="list-style-type: none"> <li>• Improved coordination along supply chain increases security</li> </ul>	<ul style="list-style-type: none"> <li>• Platform for broader alignment</li> <li>• Enable creation of a secure supply chain network for common problem solving, resource sharing</li> <li>• Improve communication among supply chain partners, potentially reducing coordination costs</li> </ul>
Proactive Technology Investments	<ul style="list-style-type: none"> <li>• Technology provides increased ability to track, monitor, and observe material flows, preventing excursions</li> </ul>	<ul style="list-style-type: none"> <li>• Ability to customize the application to the benefit of the firm</li> <li>• Increase process efficiency through technology</li> <li>• Visibility investments give real-time awareness of supply chain delays, location, and status</li> </ul>
TQM Investments	<ul style="list-style-type: none"> <li>• More consistent security procedure execution</li> <li>• Application of Six Sigma may lead to disciplined loss reduction efforts</li> <li>• Lower losses</li> <li>• Higher-performance employees emphasize security</li> <li>• Process design standardizes security processes</li> <li>• Design supply chain with fewer handoffs, keeping product moving</li> </ul>	<ul style="list-style-type: none"> <li>• Discipline increases, enabling compliance (quality, safety, process)</li> <li>• Reduction in safety stock, lead-time variance, and lower OS&amp;D</li> <li>• Better process knowledge and management from additional data, greater visibility to discern bottlenecks and congestion</li> <li>• Safety stock reduction as a result of advance lead-time information</li> <li>• Investment in quality processes results in quality security</li> <li>• Consistent process operation leads to fewer disruptions, faster and more reliable operation</li> <li>• Process discipline leads to higher levels of performance, efficiency</li> </ul>
Voluntary Security Compliance	<ul style="list-style-type: none"> <li>• European Union’s Authorized Economic Operator program ensures base level of supply chain security assessment</li> <li>• Customs specialists working in specialized security programs may observe risk of security breach before breach can occur</li> <li>• Customs-Trade Partnership Against Terrorism (C-TPAT) membership provides member companies with information about industry “best practices” in supply chain security</li> <li>• Sweden’s StairSec program leads to higher inspection rates of uncertified cargo, increasing likelihood of early warning and prevention</li> </ul>	<ul style="list-style-type: none"> <li>• Establish a “mandatory” fundamental standard across industry for supply chain security via a “voluntary” program</li> <li>• A platform for collaboration and alignment within an industry that leads to industry standards, raising overall level of performance in quality, service, and cost</li> <li>• C-TPAT supply chain specialist assists firm as CBP liaison for validation, security issues, procedural updates, communication, and training</li> <li>• Faster border throughput times from fewer inspections and “green lane” flow, which may raise service levels, enabling lower working capital</li> <li>• Process discipline enables compliance (quality, safety, process), higher levels of process performance</li> </ul>

# Endnotes

1. A number of terms have been used to describe this capability, including resilience, business continuity, contingency planning, and “trade security” (“trade security” refers to a broader set of capabilities described in the white paper “Trade Security: The New Equation for the New Normalcy” by the authors). One can think of supply chain security in terms of maintaining the integrity of the product, processes, and information, in contrast to supply chain continuity or resilience, which we define as “the ability to react to unexpected disruption and restore normal supply chain operations.”
2. Supply chain security investments range from capital equipment, human resources, process improvements, and operating expenses for a range of activities including physical security improvements, monitoring, and incident investigation.
3. This problem has also been recently addressed by researchers using system dynamics methods. See “Nobody Ever Gets Credit for Fixing Defects that Didn’t Happened: Creating and Sustaining Process Improvement,” *California Management Review*, 43, 4:64–88 by N. Repenning and J. Sterman, 2001.
4. Early mention of collateral benefits includes insights from several leaders, including Dr. Ruth David, CEO and president of ANSER Analytical Service, who coined the term “dual benefits.” Additionally, “dual benefit solutions” are profiled through the Homeland Security Institute operated by ANSER ([http://www.homelandsecurity.org/bulletin/current\\_bulletin.cfm](http://www.homelandsecurity.org/bulletin/current_bulletin.cfm)).
5. “Quality is free” by Phil Crosby. Professor Hau Lee and Michael Wolfe also recognized and noted similarities between security improvement and quality improvement in their article “Supply Chain Security without Tears” published in *Supply Chain Management Review*, Jan–Feb 2003.
6. J. Martha and S. Subbkrishna. (2002), “Targeting a just-in-case Supply Chain for the Inevitable Next Disaster,” *Supply Chain Management Review*, September/October, pp. 18–23.
7. Vinod Singhal, “Supply Chain Glitches and Shareholder Value Destruction,” *Business Briefing: Global Purchasing and Supply Chain Strategies*. In this study, the researchers examined instances where firms experienced production or shipping delays as announced in the *The Wall Street Journal* or the Dow Jones News Service.
8. Ibid.
9. Almar Latour, “Trial by Fire: A Blaze in Albuquerque Sets Off Major Crisis For Cell-Phone Giants,” *The Wall Street Journal*, January 29, 2001, page A1.
10. “The No-See-Um’s: The Financial Impact of Cargo Losses on the Bottom Line.” Presentation at the 2004 Council of Logistics Management Annual Conference on October 6, 2004, by Robert S. Holley, Chubb & Son.
11. The data was derived from an interview conducted in 2005 by Abby Benson and James B. Rice, Jr., both of MIT, as part of a study on supply chain security.
12. Examples of multiple levels of firms collaborating include sourcing personnel working with sales personnel, product development personnel working with design engineers, and warehousing managers working with distribution and shipping managers.
13. The data was derived from an interview conducted in 2005 by Abby Benson and James B. Rice, Jr., both of MIT, as part of a study on supply chain security.
14. The data was derived from an interview conducted in 2003 by Federico Caniato, Visiting Student MIT, and James B. Rice, Jr., as part of a study on supply chain resilience.
15. Hau L. Lee and Seungjin Whang, “Higher Supply Chain Security with Lower Cost: Lessons from Total Quality Management,” Stanford University white paper, October 19, 2003, p. 21.

16. Reference Benson-Rice interviews. One 3PL provider described C-TPAT as a “choiceless choice because a company that doesn’t comply will go out of business since all major importers require it.”

17. “Securing the Global Supply Chain: Customs-Trade Partnership Against Terrorism (C-TPAT) Strategic Plan,” U.S. Customs and Border Protection, April 2005.

18. The availability of “green lanes” will vary by country and their respective progress toward developing the necessary technology and infrastructure to support building “green lane” processes.

19. Ref. Benson-Rice interview.

20. Ref. Benson-Rice interview.

21. Ref. Benson-Rice interview.

22. Deena S. Disraeli, “Public-Private Partnerships: Security and Emergency Response Collaboration in a New Threat Environment,” MIT Thesis, June 2004.

23. Tobey Gooley, “C-TPAT: Separating Hype from Reality,” *Logistics Management*, August 1, 2004.

24. Ibid.

25. Data derived from a series of interviews conducted as part of the Supply Chain Response to Terrorism project at MIT; see <http://web.mit.edu/scresponse/> for additional information.

26. Ibid. Rice-Caniato interviews

## ABOUT THE AUTHORS

**James B. Rice, Jr.**, is the Director of the Integrated Supply Chain Management (ISCM) Program at the Center for Transportation and Logistics (CTL) at the Massachusetts Institute of Technology, having joined CTL in 1995. The ISCM Program is a consortium that enables companies from industry to interact with faculty and researchers across MIT on education and research in the supply chain domain.

Mr. Rice's research is on organization and supply chain design, recently focusing on how supply chains respond to disruptions (for example, terrorism), including the role of culture and the creation of collateral benefits, and on the impact of auto-ID on supply chain design. He also serves as project manager for the Supply Chain Response and the Smart Objects projects, and teaches a graduate course in supply chain management.



His written work includes published articles, such as "The RFID Journey: From Strategy to Action" upcoming in *Supply Chain Management Review*; "Building a Secure and Resilient Supply Network" in *Supply Chain Management Review*, Sept.–Oct. 2003; "Strategic Partnership: Collaboration, Alliances and the Coordination Spectrum" in *Logistics Solutions*, Issue 1 2002; "Supply Chain Versus Supply Chain: The Hype and Reality" in *Supply Chain Management Review*, Sept.–Oct. 2001; and "Spanning the Functional Boundaries Through Horizontal Process Management (HPM)" in *Supply Chain Management Review*, Fall 1997. He also contributed to the book *Surviving Supply Chain Integration* (National Academy Press, March 2000) and to a number of working papers prepared for CTL sponsors.

In addition to his role at MIT, Mr. Rice has served the community on several supply-chain-related boards and committees, including the National Research Council's Board on Manufacturing and Engineering Design (BMAED); the editorial board of *Supply Chain Management Review* and of *Supply Chain Forum: An International Journal*; the International Advisory Board of KLICT, a multi-year international research initiative funded by the government of The Netherlands; the United States Air Force Logistics Transformation Advisory Committee (chairman); and the U.S. Navy Supply Chain Practices for Affordable Naval Systems (SPANS) Technical Advisory Board.

Prior to joining MIT, Mr. Rice managed manufacturing and distribution operations at Procter & Gamble, and served as a sales and market manager at General Electric Company.

Mr. Rice earned his M.B.A. in operations and finance from the Harvard Business School, and a bachelor's degree in mechanical engineering from the University of Notre Dame.

**Philip W. Spayd** is a Research Affiliate, Center for Transportation and Logistics, Massachusetts Institute of Technology, and a founding director of Global Trade Systems, Inc. (GTS). GTS provides advice to companies on working to make the overall operation of international supply chains more efficient and better able to function with resiliency in the event of a disruption anywhere along the supply/demand axis. GTS works at the intersection of strategy and operations by helping companies ensure that their supply chain strategies support their business objectives. Prior to joining GTS in January 2004, Mr. Spayd served for 25 years with the U.S. Customs Service and the Department of Homeland Security, working in the U.S. and representing U.S. Customs globally. He was a founding director of Operation Safe Commerce, the first public/private partnership to develop mechanisms to enhance the security of international supply chains.



As the Boston director of field operations, Customs and Border Protection, Department of Homeland Security, Mr. Spayd directed the commercial and inspectional activities of approximately 1,000 Customs and Border Protection employees throughout the six New England states. The Boston field office was recognized for creating four “best practices” warranting national recognition: antiterrorism passenger examinations, antiterrorism training, interagency maritime intelligence, and Operation Safe Commerce.

Mr. Spayd was appointed Northeast regional commissioner in August 1988. Prior to that appointment, he was district director of Customs in Norfolk, Virginia, and before that, director of labor relations at Customs headquarters in Washington, D.C. He began his government career in 1973 and began work at Customs in 1978.

During the period of March through July 1998, Mr. Spayd was stationed in Sofia, Bulgaria, serving as the U.S. advisor to the Bulgarian government on counter-proliferation. He worked directly for the minister of the Interior and formed inter-governmental working groups to share intelligence and to coordinate operational planning. He directed a joint Bulgaria/Romania operation at a strategic port on the Danube River to stem the flow of weapons of mass destruction components in the region.

In 1992, Mr. Spayd received a Meritorious Executive Presidential Rank Award from President George H. W. Bush for innovative management. In 1996, he received an award from the World Customs Organization for international service in Eastern Europe. He is a Harvard Senior Executive Fellow. In April 2002, Mr. Spayd was awarded the Coalition of New England Companies for Trade (CONNECT) Person of the Year Award. He received this award for his contributions to the facilitation of international trade in New England in the face of the new security environment.

Mr. Spayd is a graduate of The Pennsylvania State University with a B.A. degree in political science and of the University of Massachusetts with an M.S. degree in labor and industrial relations.

## KEY CONTACT INFORMATION

### To contact the authors:

**James B. Rice, Jr.**

Director, Integrated Supply Chain Management  
Center for Transportation and Logistics  
Massachusetts Institute of Technology  
77 Massachusetts Avenue, Room E40-281  
Cambridge, MA 02139  
(617) 258-8584  
fax: (617) 253-4560  
e-mail: [jrice@mit.edu](mailto:jrice@mit.edu)

**Philip W. Spayd**

Global Trade Systems, Inc.  
7 Borden Road  
Scituate, MA 02066  
(781) 545-4462  
e-mail: [philip.spayd@globaltradesystems.com](mailto:philip.spayd@globaltradesystems.com)

## CENTER REPORTS AVAILABLE

### **COLLABORATION: PARTNERSHIPS AND NETWORKS**

**Leveraging Networks to Meet National Goals:** FEMA and the Safe Construction Networks (March 2002)  
William L. Waugh, Jr.

**21st-Century Government and the Challenge of Homeland Defense** (June 2002)  
Elaine C. Kamarck

**Assessing Partnerships:** New Forms of Collaboration (March 2003)  
Robert Klitgaard and Gregory F. Treverton

**Leveraging Networks:** A Guide for Public Managers Working across Organizations (March 2003)  
Robert Agranoff

**Extraordinary Results on National Goals:** Networks and Partnerships in the Bureau of Primary Health Care's 100%/0 Campaign (March 2003)  
John Scanlon

**Public-Private Strategic Partnerships:** The U.S. Postal Service-Federal Express Alliance (May 2003)  
Oded Shenkar

**The Challenge of Coordinating "Big Science"** (July 2003)  
W. Henry Lambright

**Communities of Practice:** A New Tool for Government Managers (November 2003)  
William M. Snyder and Xavier de Souza Briggs

**Collaboration and Performance Management in Network Settings:** Lessons from Three Watershed Governance Efforts (April 2004)  
Mark T. Imperial

**The Quest to Become "One":** An Approach to Internal Collaboration (February 2005)  
Russ Linden

**Cooperation Between Social Security and Tax Agencies in Europe** (April 2005)  
Bernhard Zaglmayer, Paul Schoukens, and Danny Pieters

### **E-GOVERNMENT**

**Supercharging the Employment Agency:** An Investigation of the Use of Information and Communication Technology to Improve the Service of State Employment Agencies (December 2000)  
Anthony M. Townsend

**Assessing a State's Readiness for Global Electronic Commerce:** Lessons from the Ohio Experience (January 2001)  
J. Pari Sabety and Steven I. Gordon

**Privacy Strategies for Electronic Government** (January 2001)  
Janine S. Hiller and France Bélanger

**Commerce Comes to Government on the Desktop:** E-Commerce Applications in the Public Sector (February 2001)  
Genie N. L. Stowers

**The Use of the Internet in Government Service Delivery** (February 2001)  
Steven Cohen and William Eimicke

**State Web Portals:** Delivering and Financing E-Service (January 2002)  
Diana Burley Gant, Jon P. Gant, and Craig L. Johnson

**Internet Voting:** Bringing Elections to the Desktop (February 2002)  
Robert S. Done

**Leveraging Technology in the Service of Diplomacy:** Innovation in the Department of State (March 2002)  
Barry Fulton

**Federal Intranet Work Sites:** An Interim Assessment (June 2002)  
Julianne G. Mahler and Priscilla M. Regan

**The State of Federal Websites:** The Pursuit of Excellence (August 2002)  
Genie N. L. Stowers

**State Government E-Procurement in the Information Age:** Issues, Practices, and Trends (September 2002)  
M. Jae Moon

**Preparing for Wireless and Mobile Technologies in Government** (October 2002)  
Ai-Mei Chang and P. K. Kannan

**Public-Sector Information Security:** A Call to Action for Public-Sector CIOs (October 2002, 2nd ed.)  
Don Heiman

**The Auction Model:** How the Public Sector Can Leverage the Power of E-Commerce Through Dynamic Pricing (November 2002, 2nd ed.)  
David C. Wyld

**The Promise of E-Learning in Africa:** The Potential for Public-Private Partnerships (January 2003)  
Norman LaRocque and Michael Latham

**Digitally Integrating the Government Supply Chain:** E-Procurement, E-Finance, and E-Logistics (February 2003)  
Jacques S. Gansler, William Lucyshyn, and Kimberly M. Ross

**Using Technology to Increase Citizen Participation in Government:** The Use of Models and Simulation (April 2003)  
John O'Looney

**Seaport:** Charting a New Course for Professional Services Acquisition for America's Navy (June 2003)  
David C. Wyld

**E-Reporting:** Strengthening Democratic Accountability (February 2004)  
Mordecai Lee

**Understanding Electronic Signatures:** The Key to E-Government (March 2004)  
Stephen H. Holden

**Measuring the Performance of E-Government** (March 2004)  
Genie N. L. Stowers

**Restoring Trust in Government:** The Potential of Digital Citizen Participation (August 2004)  
Marc Holzer, James Melitski, Seung-Yong Rho, and Richard Schwesler

**From E-Government to M-Government?** Emerging Practices in the Use of Mobile Technology by State Governments (November 2004)  
M. Jae Moon

## CENTER REPORTS AVAILABLE

**Government Garage Sales:** Online Auctions as Tools for Asset Management (November 2004)  
David C. Wyld

**Innovation in E-Procurement:** The Italian Experience (November 2004)  
Mita Marra

**Computerisation and E-Government in Social Security:** A Comparative International Study (May 2005)  
Michael Adler and Paul Henman

### FINANCIAL MANAGEMENT

**Credit Scoring and Loan Scoring:** Tools for Improved Management of Federal Credit Programs (July 1999)  
Thomas H. Stanton

**Using Activity-Based Costing to Manage More Effectively**  
(January 2000)  
Michael H. Granof, David E. Platt, and Igor Vaysman

**Audited Financial Statements:** Getting and Sustaining "Clean" Opinions (July 2001)  
Douglas A. Brook

**An Introduction to Financial Risk Management in Government**  
(August 2001)  
Richard J. Buttimer, Jr.

**Understanding Federal Asset Management:** An Agenda for Reform (July 2003)  
Thomas H. Stanton

**Efficiency Counts:** Developing the Capacity to Manage Costs at Air Force Materiel Command (August 2003)  
Michael Barzelay and Fred Thompson

**Federal Credit Programs:** Managing Risk in the Information Age (April 2005)  
Thomas H. Stanton

### HUMAN CAPITAL MANAGEMENT

**Profiles in Excellence:** Conversations with the Best of America's Career Executive Service (November 1999)  
Mark W. Huddleston

**Reflections on Mobility:** Case Studies of Six Federal Executives (May 2000)  
Michael D. Serlin

**Managing Telecommuting in the Federal Government:** An Interim Report (June 2000)  
Gina Vega and Louis Brennan

**Using Virtual Teams to Manage Complex Projects:** A Case Study of the Radioactive Waste Management Project (August 2000)  
Samuel M. DeMarie

**A Learning-Based Approach to Leading Change** (December 2000)  
Barry Sugarman

**Labor-Management Partnerships:** A New Approach to Collaborative Management (July 2001)  
Barry Rubin and Richard Rubin

**Winning the Best and Brightest:** Increasing the Attraction of Public Service (July 2001)  
Carol Chetkovich

**A Weapon in the War for Talent:** Using Special Authorities to Recruit Crucial Personnel (December 2001)  
Hal G. Rainey

**A Changing Workforce:** Understanding Diversity Programs in the Federal Government (December 2001)  
Katherine C. Naff and J. Edward Kellough

**Life after Civil Service Reform:** The Texas, Georgia, and Florida Experiences (October 2002)  
Jonathan Walters

**The Defense Leadership and Management Program:** Taking Career Development Seriously (December 2002)  
Joseph A. Ferrara and Mark C. Rom

**The Influence of Organizational Commitment on Officer Retention:** A 12-Year Study of U.S. Army Officers (December 2002)  
Stephanie C. Payne, Ann H. Huffman, and Trueman R. Tremble, Jr.

**Human Capital Reform:** 21st Century Requirements for the United States Agency for International Development (March 2003)  
Anthony C. E. Quainton and Amanda M. Fulmer

**Modernizing Human Resource Management in the Federal Government:** The IRS Model (April 2003)  
James R. Thompson and Hal G. Rainey

**Mediation at Work:** Transforming Workplace Conflict at the United States Postal Service (October 2003)  
Lisa B. Bingham

**Growing Leaders for Public Service** (August 2004, 2nd ed.)  
Ray Blunt

**Pay for Performance:** A Guide for Federal Managers (November 2004)  
Howard Risher

**The Blended Workforce:** Maximizing Agility Through Nonstandard Work Arrangements (April 2005)  
James R. Thompson and Sharon H. Mastracci

### INNOVATION

**Managing Workfare:** The Case of the Work Experience Program in the New York City Parks Department (June 1999)  
Steven Cohen

**New Tools for Improving Government Regulation:** An Assessment of Emissions Trading and Other Market-Based Regulatory Tools (October 1999)  
Gary C. Bryner

**Religious Organizations, Anti-Poverty Relief, and Charitable Choice:** A Feasibility Study of Faith-Based Welfare Reform in Mississippi (November 1999)  
John P. Bartkowski and Helen A. Regis

**Business Improvement Districts and Innovative Service Delivery**

(November 1999)

Jerry Mitchell

**An Assessment of Brownfield Redevelopment Policies:**

The Michigan Experience

(November 1999)

Richard C. Hula

**San Diego County's Innovation**

**Program:** Using Competition and a Whole Lot More to Improve Public Services (January 2000)

William B. Eimicke

**Innovation in the Administration of Public Airports**

(March 2000)

Scott E. Tarry

**Entrepreneurial Government:**

Bureaucrats as Businesspeople

(May 2000)

Anne Laurent

**Rethinking U.S. Environmental**

**Protection Policy:** Management

Challenges for a New Administration

(November 2000)

Dennis A. Rondinelli

**The Challenge of Innovating**

**in Government** (February 2001)

Sandford Borins

**Understanding Innovation:**

What Inspires It? What Makes

It Successful? (December 2001)

Jonathan Walters

**Government Management of**

**Information Mega-Technology:**

Lessons from the Internal Revenue Service's Tax Systems Modernization

(March 2002)

Barry Bozeman

**Advancing High End Computing:**

Linking to National Goals

(September 2003)

Juan D. Rogers and Barry Bozeman

**MANAGING FOR PERFORMANCE AND RESULTS**

**Corporate Strategic Planning in**

**Government:** Lessons from the United States Air Force

(November 2000)

Colin Campbell

**Using Evaluation to Support Performance Management:**

A Guide for Federal Executives

(January 2001)

Kathryn Newcomer and Mary Ann Scheirer

**Managing for Outcomes:** Milestone

Contracting in Oklahoma

(January 2001)

Peter Frumkin

**The Challenge of Developing Cross-Agency Measures:**

A Case Study of the Office of

National Drug Control Policy

(August 2001)

Patrick J. Murphy and John Carnevale

**The Potential of the Government**

**Performance and Results Act as a**

**Tool to Manage Third-Party**

**Government** (August 2001)

David G. Frederickson

**Using Performance Data for**

**Accountability:** The New York City

Police Department's CompStat

Model of Police Management

(August 2001)

Paul E. O'Connell

**Moving Toward More Capable**

**Government:** A Guide to

Organizational Design (June 2002)

Thomas H. Stanton

**The Baltimore CitiStat Program:**

Performance and Accountability

(May 2003)

Lenneal J. Henderson

**Strategies for Using State**

**Information:** Measuring and

Improving Program Performance

(December 2003)

Shelley H. Metzenbaum

**Linking Performance and Budgeting:**

Opportunities in the Federal Budget

Process (January 2004, 2nd ed.)

Philip G. Joyce

**How Federal Programs Use Outcome**

**Information:** Opportunities for

Federal Managers

(February 2004, 2nd ed.)

Harry P. Hatry, Elaine Morley, Shelli

B. Rossman, and Joseph S. Wholey

**Performance Leadership:** 11 Better

Practices That Can Ratchet Up

Performance (May 2004)

Robert D. Behn

**Performance Management for**

**Career Executives:** A "Start Where

You Are, Use What You Have" Guide

(October 2004, 2nd ed.)

Chris Wye

**Staying the Course:** The Use of

Performance Measurement in State

Governments (November 2004)

Julia Melkers and Katherine

Willoughby

**MARKET-BASED GOVERNMENT**

**Determining a Level Playing Field for Public-Private Competition**

(November 1999)

Lawrence L. Martin

**Implementing State Contracts for**

**Social Services:** An Assessment of

the Kansas Experience (May 2000)

Jocelyn M. Johnston and Barbara S.

Romzek

**A Vision of the Government as**

**a World-Class Buyer:** Major

Procurement Issues for the Coming

Decade (January 2002)

Jacques S. Gansler

**Contracting for the 21st Century:**

A Partnership Model (January 2002)

Wendell C. Lawther

**Franchise Funds in the Federal**

**Government:** Ending the Monopoly

in Service Provision (February 2002)

John J. Callahan

**Making Performance-Based**

**Contracting Perform:** What the

Federal Government Can Learn from

State and Local Governments

(November 2002, 2nd ed.)

Lawrence L. Martin

**Moving to Public-Private**

**Partnerships:** Learning from

Experience around the World

(February 2003)

Trefor P. Williams

**IT Outsourcing:** A Primer for Public

Managers (February 2003)

Yu-Che Chen and James Perry

**The Procurement Partnership Model:**

Moving to a Team-Based Approach

(February 2003)

Kathryn G. Denhardt

## CENTER REPORTS AVAILABLE

**Moving Toward Market-Based Government:** The Changing Role of Government as the Provider (March 2004, 2nd ed.)  
Jacques S. Gansler

**Transborder Service Systems:** Pathways for Innovation or Threats to Accountability? (March 2004)  
Alasdair Roberts

**Competitive Sourcing:** What Happens to Federal Employees? (October 2004)  
Jacques S. Gansler and William Lucyshyn

**Implementing Alternative Sourcing Strategies:** Four Case Studies (October 2004)  
Edited by Jacques S. Gansler and William Lucyshyn

**Designing Competitive Bidding for Medicare** (November 2004)  
John Cawley and Andrew B. Whitford

### TRANSFORMATION OF ORGANIZATIONS

**The Importance of Leadership:** The Role of School Principals (September 1999)  
Paul Teske and Mark Schneider

**Leadership for Change:** Case Studies in American Local Government (September 1999)  
Robert B. Denhardt and Janet Vinzant Denhardt

**Managing Decentralized Departments:** The Case of the U.S. Department of Health and Human Services (October 1999)  
Beryl A. Radin

**Transforming Government:** The Renewal and Revitalization of the Federal Emergency Management Agency (April 2000)  
R. Steven Daniels and Carolyn L. Clark-Daniels

**Transforming Government:** Creating the New Defense Procurement System (April 2000)  
Kimberly A. Harokopus

**Trans-Atlantic Experiences in Health Reform:** The United Kingdom's National Health Service and the United States Veterans Health Administration (May 2000)  
Marilyn A. DeLuca

**Transforming Government:** The Revitalization of the Veterans Health Administration (June 2000)  
Gary J. Young

**The Challenge of Managing Across Boundaries:** The Case of the Office of the Secretary in the U.S. Department of Health and Human Services (November 2000)  
Beryl A. Radin

**Creating a Culture of Innovation:** 10 Lessons from America's Best Run City (January 2001)  
Janet Vinzant Denhardt and Robert B. Denhardt

**Transforming Government:** Dan Goldin and the Remaking of NASA (March 2001)  
W. Henry Lambricht

**Managing Across Boundaries:** A Case Study of Dr. Helene Gayle and the AIDS Epidemic (January 2002)  
Norma M. Riccucci

**Managing "Big Science":** A Case Study of the Human Genome Project (March 2002)  
W. Henry Lambricht

**The Power of Frontline Workers in Transforming Government:** The Upstate New York Veterans Healthcare Network (April 2003)  
Timothy J. Hoff

**Making Public Sector Mergers Work:** Lessons Learned (August 2003)  
Peter Frumkin

**Efficiency Counts:** Developing the Capacity to Manage Costs at Air Force Materiel Command (August 2003)  
Michael Barzelay and Fred Thompson

**Managing the New Multipurpose, Multidiscipline University Research Centers:** Institutional Innovation in the Academic Community (November 2003)  
Barry Bozeman and P. Craig Boardman

### 2004 PRESIDENTIAL TRANSITION SERIES

**Government Reorganization:** Strategies and Tools to Get It Done (August 2004)  
Hannah Sistare

**Performance Management for Political Executives:** A "Start Where You Are, Use What You Have" Guide (October 2004)  
Chris Wye

**Becoming an Effective Political Executive:** 7 Lessons from Experienced Appointees (January 2005, 2nd ed.)  
Judith E. Michaels

**Getting to Know You:** Rules of Engagement for Political Appointees and Career Executives (January 2005)  
Joseph A. Ferrara and Lynn C. Ross

### SPECIAL REPORTS

**Enhancing Security Throughout the Supply Chain** (April 2004)  
David J. Closs and Edmund F. McGarrell

**Assessing the Impact of IT-Driven Education in K-12 Schools** (May 2005)  
Ganesh D. Bhatt

**Investing in Supply Chain Security:** Collateral Benefits (May 2005)  
James B. Rice, Jr., and Philip W. Spayd

### CENTER FOR HEALTHCARE MANAGEMENT REPORTS

**The Power of Frontline Workers in Transforming Healthcare Organizations:** The Upstate New York Veterans Healthcare Network (December 2003)  
Timothy J. Hoff

**IT Outsourcing:** A Primer for Healthcare Managers (December 2003)  
Yu-Che Chen and James Perry

## BOOKS\*

***Collaboration: Using Networks and Partnerships***

(Rowman & Littlefield Publishers, Inc., 2004)  
John M. Kamensky and Thomas J. Burlin, editors

***E-Government 2001***

(Rowman & Littlefield Publishers, Inc., 2001)  
Mark A. Abramson and Grady E. Means, editors

***E-Government 2003***

(Rowman & Littlefield Publishers, Inc., 2002)  
Mark A. Abramson and Therese L. Morin, editors

***Human Capital 2002***

(Rowman & Littlefield Publishers, Inc., 2002)  
Mark A. Abramson and Nicole Willenz Gardner, editors

***Human Capital 2004***

(Rowman & Littlefield Publishers, Inc., 2004)  
Jonathan D. Breul and Nicole Willenz Gardner, editors

***Innovation***

(Rowman & Littlefield Publishers, Inc., 2002)  
Mark A. Abramson and Ian Littman, editors

***Leaders***

(Rowman & Littlefield Publishers, Inc., 2002)  
Mark A. Abramson and Kevin M. Bacon, editors

***Learning the Ropes: Insights for Political Appointees***

(Rowman & Littlefield Publishers, Inc., 2005)  
Mark A. Abramson and Paul R. Lawrence, editors

***Managing for Results 2002***

(Rowman & Littlefield Publishers, Inc., 2001)  
Mark A. Abramson and John M. Kamensky, editors

***Managing for Results 2005***

(Rowman & Littlefield Publishers, Inc., 2004)  
John M. Kamensky and Albert Morales, editors

***Memos to the President: Management Advice from the Nation's Top Public Administrators***

(Rowman & Littlefield Publishers, Inc., 2001)  
Mark A. Abramson, editor

***New Ways of Doing Business***

(Rowman & Littlefield Publishers, Inc., 2003)  
Mark A. Abramson and Ann M. Kieffaber, editors

***The Procurement Revolution***

(Rowman & Littlefield Publishers, Inc., 2003)  
Mark A. Abramson and Roland S. Harris III, editors

***Transforming Government Supply Chain Management***

(Rowman & Littlefield Publishers, Inc., 2003)  
Jacques S. Gansler and Robert E. Luby, Jr., editors

***Transforming Organizations***

(Rowman & Littlefield Publishers, Inc., 2001)  
Mark A. Abramson and Paul R. Lawrence, editors





### **About the IBM Center for The Business of Government**

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion on new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

The Center is one of the ways that IBM seeks to advance knowledge on how to improve public sector effectiveness. The IBM Center focuses on the future of the operation and management of the public sector.

### **About IBM Business Consulting Services**

With consultants and professional staff in more than 160 countries globally, IBM Business Consulting Services is the world's largest consulting services organization. IBM Business Consulting Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build and run those solutions in a way that delivers bottom-line business value. For more information visit [www.ibm.com/bcs](http://www.ibm.com/bcs).

### **For additional information, contact:**

#### **Mark A. Abramson**

Executive Director

IBM Center for The Business of Government

1301 K Street, NW

Fourth Floor, West Tower

Washington, DC 20005

(202) 515-4504, fax: (202) 515-4375

e-mail: [businessofgovernment@us.ibm.com](mailto:businessofgovernment@us.ibm.com)

website: [www.businessofgovernment.org](http://www.businessofgovernment.org)