Special Report Series

Enhancing Security Throughout the Supply Chain

David J. Closs
John H. McConnell Chair in Business Administration
Department of Marketing and Supply Chain
Management
Michigan State University

Edmund F. McGarrell
Director and Professor
School of Criminal Justice
Michigan State University

IBM Center for
**The Business
of Government**

Enhancing Security Throughout the Supply Chain

David J. Closs
John H. McConnell Chair in Business Administration
Department of Marketing and Supply Chain Management
Michigan State University

Edmund F. McGarrell
Director and Professor
School of Criminal Justice
Michigan State University

April 2004

T A B L E   O F   C O N T E N T S

F O R E W O R D

April 2004

On behalf of the IBM Center for The Business of Government, we are pleased to present this report, "Enhancing Security Throughout the Supply Chain," by David J. Closs and Edmund F. McGarrell.

Major events over the past couple of years, including 9/11, the San Francisco port lockout, Hurricane Mitch, SARS, and the recent blackout in the northeastern United States and Canada, have dramatized the vulnerability of the global supply chain. These events, together with trends of increased outsourcing, under- score the need for companies to be more diligent in the way they manage their own extended supply chain, ensuring resiliency of operations end to end. That means addressing all aspects of their operations, from working with global suppliers and balancing supply/demand to improving overall security.

Specifically in the area of security, the protection of goods and commodities as they travel through the supply chain poses unique challenges. The report by Professors Closs and McGarrell describes many of the supply chain security challenges that exist today. It highlights the issues governments and firms will face as they attempt to build greater security into the global supply chain, and offers practical and strategic advice for how to use investments in new security programs to improve the efficiency and flexibility of the supply chain.

Their report asserts that companies and governments must recognize the need to implement comprehensive and integrated end-to-end security that extends beyond asset protection and prevents the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain. It also contends that organizations should be looking strategically at security and how investments there can create oppor- tunities to build flexibility into their businesses through new processes that give them as early a warning as possible of any interruptions.

Taking a strategic view of security, this report helps businesses focus on the benefits—not just the costs— associated with implementing supply chain security measures. By increasing supply chain security, compa- nies will see new opportunities for cost savings, have greater visibility for better planning, and be able to forge closer relationships with trading partners—all of which can provide them with a significant advantage over competitors who may not be taking the same approach.

This document is based on the results of research and a multi-organizational, cross-functional workshop held in November 2003. A high-level checklist was also developed to assist companies and governments in assessing the status of their supply chain security and in determining the risks associated with their performance in each category.

We trust that this report will serve as the catalyst for the new thinking, sustained leadership, research, and continual learning required by both the public and private sectors to sustain the global supply chain security needed today and in the future. Supply chain security case studies will help refine the assessment checklist and recommended actions described in this report. Clearly, much work remains to be done.

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

Patrice N. Knight
Vice President
Import Compliance Office
IBM Corporation
knighp@us.ibm.com

EXECUTIVE SUMMARY

Global supply chain security has become increasingly important due to incidents involving damage, theft, and terrorism. While security has been the primary focus of a number of institutions involved in supply chain operations (firms, governments, carriers, and the consuming public), it has traditionally received a functional focus. For example, firms' security organizations primarily focused on asset security while the government focused on revenue collection and restricting the flow of illegal items. In order to effectively meet the demands of a secure supply chain in today's environment, a more comprehensive and integrated security focus is required, extending beyond asset protection and preventing the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain.

This report synthesizes the results of research and a multi-organizational cross-functional workshop sponsored by IBM and held at Michigan State University (MSU) in November 2003. The workshop included representatives from manufacturers, distributors, retailers, carriers, government, and academia. The report is designed to meet five objectives:

- To establish some common definitions regarding supply chain management and security.

- To describe the broad perspective that is necessary for comprehensive supply chain security management.

- To review the critical dimensions and requirements for supply chain security.

- To introduce an assessment tool for firms, governments, carriers, and terminal/port operators to benchmark themselves against other institutions involved in enhancing supply chain security.

- To propose recommendations, synthesized from MSU research and the workshop, that are critical for enhancing supply chain security effectiveness. These recommendations suggest the need for enhanced leadership; public-private collaboration; additional research for supply chain security, policy making and application planning; and educational initiatives to develop awareness and expertise.

The central thesis of this document is that both security and supply chain efficiencies can be maximized, but to do so will require changes in thinking, sustained leadership, and continual learning in both the public and private sectors.

Introduction

About the Report

This report introduces the concept of supply chain security management and offers guidelines for its implementation. The first section characterizes the shift of supply chain security from a focus on asset protection to one of process integrity that prevents the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain.

It emphasizes the need to consider the institutions and activities required to move the product from the field, forest, or mine to the home or office. While the need for enhanced supply chain security is apparent, the challenge is for firms to provide improved security capabilities at minimal to no increase in cost.

The second section reviews the goals of effective supply chain management. While the goal is to continue providing increased customer value through high velocity and visibility, the firm and its supply chain partners must refine their processes to reduce variability and vulnerability. Effective supply chain security management requires a thorough knowledge regarding these trade-offs. This section also suggests that supply chain security initiatives reflect an extension of the quality movement. While the quality movement focused on product and production process, supply chain security requires cross-organization process and information integration.

The third section describes an assessment approach that can be used to evaluate and benchmark firm and institutional supply chain security management practices. While this assessment provides firms with the insight to enhance their own supply chain security capabilities, a comprehensive security solution requires more involvement of all organizations involved in supply chain planning, execution, control, and monitoring.

The final section describes the institutional roles and recommendations required to develop a comprehensive approach to enhancing global supply chain security. A firm or even an entire supply chain cannot solve domestic or global security problems on its own. Comprehensive supply chain security requires a partnership involving firms, supply chain partners, service providers, and government. This report describes the institutional relationships, objectives, requirements, and best practice characteristics. Its ultimate goal is to enhance global supply chain security through leadership, collaboration, research, and education.

About the Challenge of Enhancing Supply Chain Security

The dawn of the 21st century brought together a variety of factors that created a need for enhanced supply chain security. First, the increasingly global economy both generates and depends on the free flow of people, goods, and information. Second, businesses increasingly depend on efficient supply chain operations. Third, increased terrorist threats result in significant implications for homeland and global security. These factors have created significant challenges for businesses, for the country, and for the global economy. Simply put, firms must

implement continuous improvement processes that enhance *both* supply chain execution and security.

Improvements must go beyond the firm itself and extend throughout the supply chain. At the same time, governmental agencies responsible for the movement of goods and people across borders must continuously review and update security procedures with the goal of enhancing both security and effi-ciency. This includes balancing the essential govern-mental obligation to protect citizens with the critical role of promoting economic viability through trade. Further, the focus must be global, with the goal of expanding the number of trusted partners to enhance global trade. Failure to enhance security—as demonstrated by terrorist attacks in Bali, Israel, Kenya, Saudi Arabia, Spain, Tanzania, and the United States, among others—carries unacceptable risk. Yet, enhanced security must be balanced by the efficient and synchronized flow of goods and information throughout the supply chain.

Prior to discussing the challenges, it is useful to establish common definitions for supply chains and supply chain security. A *supply chain* is the combi-nation of organizations and service providers that manage the raw material sourcing, manufacturing, and delivery of goods from the source of the com-modities to the ultimate users. Organizations directly involved in the supply chain include raw material providers such as mines, farms, manufacturers that enhance the value of raw materials, wholesalers, distributors, and retailers. Other stakeholders involved with supply chain operations include governments, carriers, and terminal/port operators. *Supply chain management* is the inter- and intra-organizational coordination of the sourcing, pro-duction, inventory management, transportation, and storage functions with the objective of meeting the service requirements of consumers or users at the minimum cost. *Supply chain security manage-ment* is the application of policies, procedures, and technology to protect supply chain assets (product,

facilities, equipment, information, and personnel) from theft, damage, or terrorism, and to prevent the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain.

The challenges facing the public and private sectors become apparent when one considers the extent of global trade. Over 200 million containers are shipped between the world's seaports annually. The United States receives approximately 17,000 con-tainers per day (Lee and Whang 2003). Only about 2 percent of the containers imported are physically inspected (Gillis 2002 and 2003). The impracticality of drastically increasing physical inspection, coupled with concerns over the security of containers, has led U.S. Customs to develop the Container Security Initiative (CSI), which moves risk assessment and inspection to earlier stages in the supply chain.

The need for heightened supply chain security was apparent in the May 2002 theft of a truck in Mexico reportedly carrying eight tons of cyanide, which resulted in a two-week search by law enforcement before the shipment was located. This incident high-lighted the potential threat posed by the movement of hazardous materials as well as the advantages that would accrue through a combination of improved security practices and tracking technology.

Challenges were also highlighted by the diagnoses of foot-and-mouth disease in the United Kingdom, "mad cow disease" in Canada, and bird flu in Asia. The December 2003 announcement of mad cow disease *(bovine spongiform encephalopathy)* in the United States was quickly greeted with the clo-sure of beef exports to many U.S. trade partners. Agriculture officials began the process of tracing back the movement of the cow and of other cows that may have fed from the same feedlot as the infected cow. This incident dramatically demon-strated the need to be able to trace the movement of goods (cattle) throughout the food supply chain.

The goal of terrorist events is to bring our economy to a standstill. If we put an anti-terrorist mindset on and make the protocol extremely cumbersome to avoid the terrorist event, we risk achieving the same outcome the terrorists desire.

—Stephen Zujkowski, senior vice president, Savi Technology (cited in Hannon 2002)

Acronyms

ACI	Advance Cargo Information
AMR	Advanced Manifest Rule
CSI	Container Security Initiative
C-TPAT	Customs-Trade Partnership Against Terrorism
DHS	Department of Homeland Security
FAST	Free and Secure Trade
ISO	International Organization for Standardization
RFID	Radio Frequency Identification
SCEM	Supply Chain Event Management
SST	Smart and Secure Tradelanes
TAPA	Technology Asset Protection Association
WCO	World Customs Organization
WTO	World Trade Organization

The report begins with a discussion of the necessary shifts in thinking, noting particularly the scope of public-private institutional partners responsible for supply chain security. The next section covers the dimensions of supply chain security. The intent is to assist all those responsible for supply chains by providing a common language and a set of principles, referred to as the five "V's," that are essential for supply chains. The report also includes an assessment tool intended to help frame issues, assist firms, and stimulate movement toward systematic metrics. Finally, recommendations are offered to place the issue of global supply chain security at the top of national and international security agendas and to promote the development and implementation of secure and efficient global supply chains.[1]

At the same time, it highlighted the potential disruption of agricultural and food markets unless suspect products can be quickly traced and isolated.

New security measures following September 11, 2001, are estimated to cost the U.S. economy alone over $150 billion, of which $65 billion is for changes in supply chains (Bernasek 2002; Damas 2001). Yet, despite these expenditures, concerns about the security of goods crossing global borders remain and the threat of terrorist attacks that could shut down borders and seriously damage the global economy remains ever present.

The purpose of this report is to highlight the issues facing all stakeholders in global trade as countries and firms attempt to build greater security into the global supply chain while simultaneously working to enhance the efficient flow of goods and services. *The guiding thesis is that both security and supply chain efficiencies can be maximized, but to do so will require changes in thinking, sustained leadership, and continual learning in both the public and private sectors.* For the government official, the desired outcome is to be able to say, "We have increased security to maximize the protection of our citizens while facilitating the efficient movement of goods across borders." For the CEO, the desired goal is to be able to say, "We are better off competitively because of our investments in supply chain security."

Understanding Supply Chain Security

New Ways of Thinking About Supply Chain Security

The supply chain security challenges posed by the threat of terrorism have significant implications for firms and their suppliers, customers, carriers, terminal operators, governments, and global partners. Indeed, the global economy is dependent on the security and resiliency of supply chains. *Supply chain resiliency* refers to the supply chain's ability to withstand and recover from an incident. A resilient supply chain is proactive—anticipating and establishing planned steps to prevent and respond to incidents. Such supply chains quickly rebuild or re-establish alternative means of operations when the subject of an incident.

For *firms,* no longer is it adequate to focus on internal security procedures geared toward the prevention of theft and emergency planning for specific plant locations and distribution centers, the so-called "four walls" perspective. Rather, the demands of supply chain security extend beyond theft prevention to the threat of terrorism and require the integration of security with many other units. Thus, for example, several firms at the Supply Chain Security Workshop held at Michigan State University in November 2003 reported the use of a cross-functional team composed of Tax Staff, Customs, Security, Government Relations, Production Control and Logistics, Purchasing, Internal Controls, and Human Resources. *Not only must firms be concerned about security procedures within their own processes and those of first-tier suppliers, but also they are dependent on the security procedures throughout the entire supply chain.*

Given the global nature of supply chains, firms are similarly dependent on the procedures, laws, and regulations of countries across the globe, and decisions about suppliers are likely to increasingly depend on the "trusted partner" status of the supplier country. Finally, supply chain managers must engage in self-appraisal of supply chain security and contingency planning, and cross-functional teams must develop crisis management plans that include planning, mitigation, detection, and response and recovery components (see Supply Chain Security Assessment beginning on page 18).

Governments are responsible for facilitating the movement of people and goods across borders and are ultimately responsible for the safety of people, the country, and commerce. For governments and government agencies, the traditional focus has been on the control of trade, ensuring the collection of taxes and fees, restricting the flow of illegal items, with sampling inspections of imports for security.[2] The contemporary focus, however, is shifting to trade facilitation with security concentrated on earlier stages in the supply chain and the identification of trusted partners to increase security through export inspection and information trails. The very notion of trusted partners, however, creates the need for global cooperation.

The United States and many of its trading partners have responded to the threat of terrorism by initiating a number of efforts to build security and facilitate trade. Congress mandated that the Department of Homeland Security (DHS) Directorate of Border and Transportation Security ensure the speedy,

We aren't necessarily replacing the focus on asset protection, but broadening it to include other considerations. The current focus on asset protection tends to be myopic; what is needed is broader language, and a recognition that when the supply chain is cut off, it affects the pipeline for all stakeholders, all resources. Perhaps we need to consider our "assets" in a context of our ability to satisfy our customers and maintain our reputation in the marketplace. That brings supply chain security into the conversation.

—Supply Chain Security Workshop, Michigan State University, November 17, 2003

orderly, and efficient flow of lawful traffic and commerce (Russell and Saldanha 2003). U.S. Customs and Border Protection, now part of DHS, has attempted to facilitate trade and increase security through the Customs-Trade Partnership Against Terrorism (C-TPAT), Container Security Initiative (CSI), and related programs. C-TPAT seeks to certify known shippers through self-appraisals of security procedures coupled with Customs audits and verifications. CSI calls for pre-screening of containers coupled with fast tracking when the cargo reaches the United States. The Advanced Manifest Rule (AMR) and more recent Advance Cargo Information (ACI) require detailed cargo data before the cargo is brought into or shipped from the United States by ocean, air, rail, or truck.[3] The Free and Secure Trade (FAST) program allows low-risk goods transported by trusted carriers for trusted firms to pass rapidly through border crossings while reserving inspection resources for unknown or high-risk shipments. These provisions all require international cooperation. Also evolving is the creation and use of technology to enhance the detection of tampering, increase tracking efficiency and effectiveness, and extend the scope of trusted partners to increase efficiency at a greater number of shipping locations.

These global efforts are not confined to the initiatives of the U.S. government. The World Trade Organization (WTO) also seeks to facilitate trade by moving controls and inspection to the export stage and through the sharing of uniform information among government agencies, firms, suppliers, carriers, and customers (Damas 2002). The World Customs Organization (WCO), through the 161 member countries involved in the Global Standards for Supply Chain Security initiative, similarly seeks to promote trade facilitation by developing and promoting guidelines to help customs administrations work together to promote rapid clearance of low-risk cross-border shipments.

The U.S. Customs programs as well as the efforts of the WTO and WCO have broadened customs verification processes to include exports, relying on declarations that include essential data for adequate cargo risk assessment (commodity description, price, origin and destination, shipper and consignee, and transportation provider) (Gillis 2003) and by certifying manufacturers, carriers, and other entities. The International Organization for Standardization (ISO) is working with the Strategic Council on Security Technology on a Smart and Secure Tradelanes (SST) initiative. SST is developing a technology platform to track containers globally and generate chain-of-custody audit trails (Hickey 2003).

Until we find a way to enable people to share information freely, compliance will remain a cat-and-mouse game in which the primary goal is to get the green light and move on. Developing a true collaborative partnership between the public and private sectors will require the creation of true two-way intelligence.

—Supply Chain Security Workshop, Michigan State University, November 17, 2003

The goal is to create global data exchange that allows all members of a supply chain to work together, creating an environment similar to that of the quality initiatives in the early 1990s. At that time, consumers were demanding substantially increased product and service quality. The result was a strong organizational focus on efforts to increase product and process quality. While firms initially felt that they could increase prices to cover the cost of quality improvements, the market quickly indicated that it would be necessary to increase quality without corresponding price increases. In fact, many firms found it was possible to increase quality while reducing cost. Similarly, it is important to note that enhanced supply chain security is expected with no increase in cost. Thus, the challenge today is to review, refine, and extend existing supply chain practices to provide the desired security controls while simultaneously lowering supply chain cost.

Firms, governments, and governmental associations are only some of the institutional components of the supply chain. The loss of a key *supplier* can critically disrupt a supply chain, and firms are dependent on the security procedures of suppliers in order to insure their own security and to maintain trusted-partner status with government agencies. *Customers* are obviously the end point of the supply chain, and thus firms are ultimately dependent on their satisfaction. Customers are also important in the sense that the information needed to

allow auditing of cargo movement from supplier to customer must extend to the customer stage. Food and product recalls linked to imminent danger are perhaps the best examples of this requirement.

Carriers, freight forwarders, port authorities, and *terminal operators* are responsible for critical stages in the supply chain process. The best procedures of a trusted trading partner are meaningless absent the effective security procedures of carriers to secure goods in transit. In addition to being key points for inspection, port facilities are potential targets for terrorists seeking to disrupt the supply chain either through attacks on the facility or as infiltration points for cargo tampering. Consequently, the entire supply chain is dependent on the security procedures (e.g., access control, personnel screening, physical "four wall" security, emergency preparedness) of port authorities and carriers and for their effective interaction with governmental agencies.

Summary: These shifts in thinking about security are captured in Figure 1. To build supply chain security, no longer can the security function be isolated from other business processes. Rather, security and efficiency must be the responsibility of cross-functional teams. These teams must be focused not only on theft and asset protection but also on preventing the use of shipments for the conveyance of contraband and weapons of mass destruction. The inadvertent shipment of such contraband poses threats not only to the firm but

Figure 1: Import Compliance Model of Changing Supply Chain Security Requirements

From	To
Corporate Security	Cross-Functional Team
Theft Prevention	Theft Prevention *and* Anti-Terrorism
Inside the Company	End-to-End Supply Chain
Vertically Integrated Supply Chain 1st Tier Suppliers	Outsourced Business Model 2nd, 3rd Tier Suppliers
Country or Geographic Focus	Global Focus
Contingency Planning	Contingency Planning *and* Crisis Management
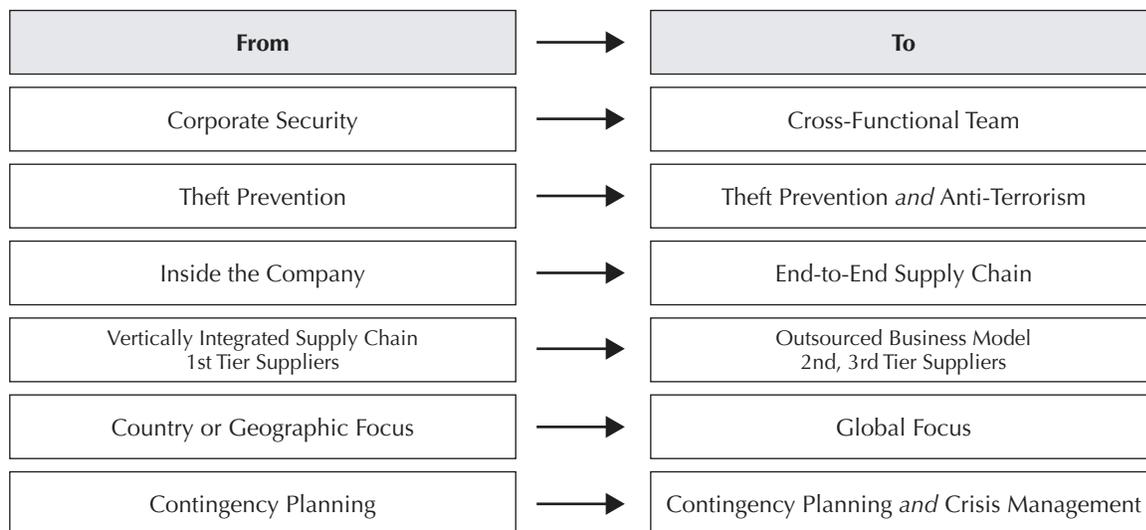
also to global trade generally. Attention must be directed to the entire supply chain, and all of these efforts—whether examined at the firm level or at the level of international government associations—require public-private communication, cooperation, and collaboration.

Dimensions of Security

Figure 2 illustrates some of the institutions that play critical roles within the supply chain. The supply chain security challenge is to effectively manage the "Five V's" across the top of the figure (Helferich and Cook 2003). The first challenge is to provide the consumer with better *value* in return for their money. Consumers expect relatively stable prices and have low tolerance for dramatic increases or variations due to supply chain security require-ments. Enhanced supply chain *velocity* is the sec-ond challenge faced by the linked members of a typical supply chain today. Not only do initiatives to increase product velocity in the supply chain reduce cost by reducing product storage times and damage, such velocity also results in better quality because products spend less time in storage facili-ties and transportation equipment. Velocity also limits the exposure to terrorist threats as it reduces the time that the product is stationary.

The third challenge is to reduce supply chain *variability*. Most supply chains commonly experi-ence variability in production and transit times. Variations in production and transit time result in larger inventory buffers or safety stocks. For exam-ple, if the average transit time from a West Coast producer to the East Coast market is five days but actual movement time varies from three to 10 days, a five-day buffer stock is required at the destination to accommodate the variation. The buffer stock results in lower velocity, higher cost, and greater potential product quality and security problems. The fourth challenge is to provide appropriate sup-ply chain *visibility*. Many supply chain participants can leverage visibility to resolve problems caused by supply chain variation. Visibility regarding where a product is in the supply chain and positive tracking to determine arrival gives manufacturers, wholesalers, or retailers a chance to expedite the product or obtain it from an alternative source.

The final challenge is to manage supply chain *vulnerability*. Supply chain vulnerability exists in a variety of forms. An obvious form in the food sup-ply, for example, is product infection or infestation with a biochemical agent at any point within the supply chain. Less obvious forms include damage or destruction of the supply chain infrastructure or

Figure 2: Supply Chain Network—The Challenges
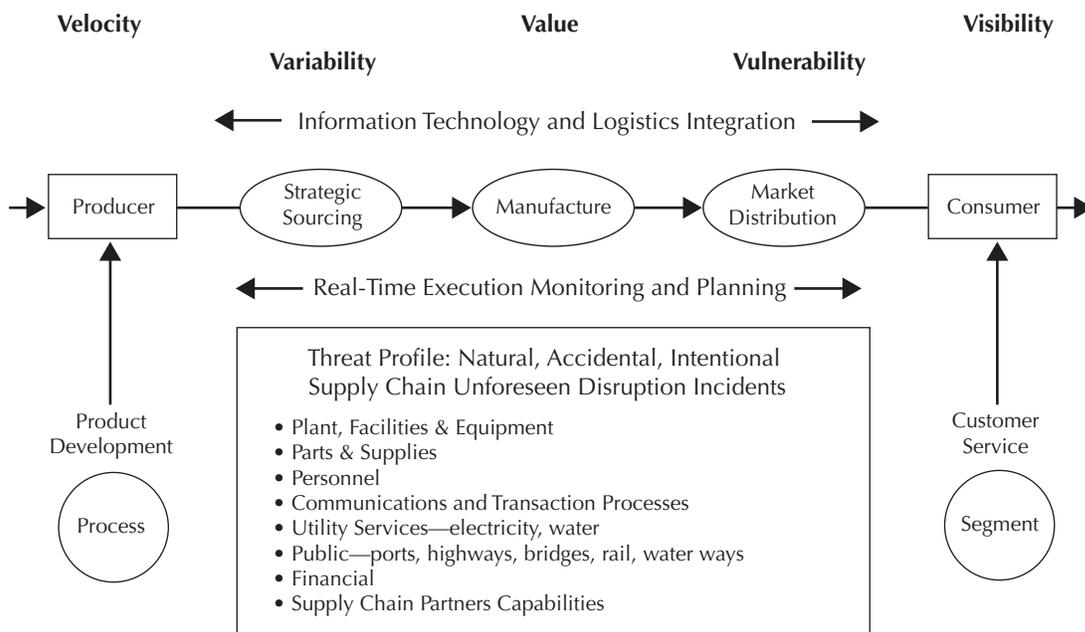
Source: Adapted from Helferich and Cook 2003.

of the processes used to move and store the product from the supplier to the customer. Examples include systematic damage or destruction to critical material suppliers, transportation equipment, transport infrastructure, storage facilities, or information processing systems. Such damage was experienced by firms, suppliers, customers, and carriers in the aftermath of September 11, when borders were closed, air transport shut down, and inventories rapidly depleted.

Effective and efficient supply chains require the balancing of the five "V" elements to provide consumer value while minimizing the cost and threat vulnerability. This balancing must incorporate the multiple perspectives of consumers, firms, government, and the public. From an institutional perspective, this includes producers, material suppliers, manufacturers, wholesalers, distributors, retailers, and carriers. From a capability perspective, this includes individuals with skills in sourcing, manufacturing, inventory management, packaging, warehousing, transportation, and security as well as support sciences (e.g., biochemical sciences).

A critical component of the global supply chain, indeed the context within which supply chains exist (represented in Figure 2), is the role of government and the relationship between governments and the private sector. Whereas governments must balance the goals of security and trade facilitation—and are ultimately dependent on the cooperation of the private sector—suppliers, firms, carriers, and other stakeholders in supply chains must recognize that international trade is a privilege granted by governments. Thus, the global economy ultimately is dependent on the mutual

obligations of both the public and private sectors, with both of them needing to strengthen supply chain security.

Integrated Supply Chain Security

The need for supply chain security is apparent from a variety of perspectives. From a traditional asset protection viewpoint, the value of goods being shipped in a single ship, plane, or truck can be enormous. One van stolen at London's Heathrow Airport carried computer chips valued at $10 million, and Jonathan Littman (2003) estimates that a small truck or van can easily carry $10 million in cargo. Worldwide cargo theft is estimated at over $50 billion annually (National Cargo Security Council as cited in Littman). However, supply chain security initiatives must extend beyond just asset protection. A secure supply chain must guarantee shipment integrity throughout the supply chain. This includes:

- Not allowing any biological or chemical agent to be introduced to the product.

- Not allowing any illegal commodity to be intermingled with the shipment.

- Not allowing the replacement of the product with an illegal commodity or person.

- Not allowing the shipment to be used as a weapon.

The focus on asset protection expands when the firm considers the security of its people, facilities, and processes globally. The disruption of a key operation has the potential of rippling through the supply chain and disrupting processes based on just-in-time inventory. Beyond the firm, the security procedures

---

The Customs-Trade Partnership Against Terrorism (C-TPAT) represents an important start toward collaboratively addressing the issues of supply chain security; however, there are many entities that need to be coordinated, and it is easy to find weaknesses in the current system. Despite all the planning and technology that has been applied, we will still be in "organized chaos" in the event of a critical disruption of the supply chain. For one thing, we need to become clearer about the dual strategies of 1) mitigating risk, and 2) creating a resilient and efficient supply chain.

—Workshop on Supply Chain Security, Michigan State University, November 17, 2003

We applaud the efforts that are underway to instill quality processes, to inspect products and containers at the points of origin, to use technology to automate the chain of custody, to monitor the process closely during the transportation journey, and to create transparency and visibility across the supply chain. Informational, rather than physical, activities form the core of security measures.

—Lee and Whang (2003: 26)

of suppliers and carriers become critical for the efficient movement of goods. The picture grows even more complex when one considers that this movement of goods is dependent on procedures, policies, and practices consistent with governmental practices intended to increase the security of borders.

The focus on balancing the five "V" elements of supply chain security on a global scale points to the need for integrated supply chain security. This is a shift from traditional security perspectives that have tended to be focused within the "four walls" of the plant or facility and asset protection focused.

Russell and Saldanha's Five Tenets of Security-Aware Logistics and Supply Chain Operation

Tenet 1: Companies need to partner with local, state, and federal government organizations that impact the movement of freight.

Tenet 2: Now more than ever, companies need to know their overseas trading partners and take responsibility for securing their cross-border supply chains.

Tenet 3: Companies need a mode-shifting capability to accommodate unexpected delays, interruptions, and disasters.

Tenet 4: Companies need to develop a suite of communication channels and media to manage crises.

Tenet 5: There is a need to adopt the military concepts of agility, reservists, and pre-positioning for the management of business logistics and the supply chain in the new environment.

Source: Russell and Saldanha 2003.

Requirements for Supply Chain Security

It is estimated that as many as 25 different parties are involved in the global movement of a container (buyers, sellers, inland freighters, shipping lines, middlemen [e.g., customs and cargo brokers], financiers, government) (Russell and Saldanha 2003). Thus, secure and efficient supply chains must be cross-institutional, including producers, material suppliers, manufacturers, wholesalers, distributors, retailers, and carriers. As has been stressed repeatedly, they must be global and they must enhance both security and efficiency.

In many respects, the shifts in thinking required for supply chain security are very similar to the paradigm shifts that occurred in the quality movement. Gaining efficiencies while ensuring security is very similar to the quality movement principle that "higher quality can be attained at lower cost by proper management and operational design" (Lee and Whang 2003: 4). Just as quality management rejected "sampling inspection" at the end of the product line and sought to build quality into all aspects of process, supply chain security will not rely on sampling inspections but rather will be the product of building security and efficiency throughout the supply chain (Lee and Whang 2003). The parallels to the quality movement and the shifts in thinking required for true supply chain security are reflected in Table 1.

Finally, just as expenditures in quality proved to be a smart investment, supply chain security investments will be facilitated by demonstrating return on investment (ROI). Here promising signs are emerging. A number of firms participating in the Supply Chain Security Workshop at Michigan State University report that investments in supply chain security were already yielding ROI (although they

Table 1: Lee and Whang's Model of Supply Chain Security and Quality

Quality Movement	Security Initiatives
Defects are very costly	Security gaps create big risks
Total quality management	Improvement of all stakeholders
Emphasis on prevention and Poka-Yoke methods[4]	C-TPAT, CSI, sealing, and anti-tamper technologies
Source inspection	CSI and inspection at origin
Process control	Automated chain of custody
Six-Sigma cycle to identify, track, and improve	Container tracking and total visibility
Root cause analysis	Profiling system for shipments, shippers, carriers, trade routes
"Quality is free"	Higher supply chain security at lower cost

Source: Lee and Whang 2003.

also report challenges in measuring ROI). Many firms and carriers that have increased security and tightened processes have witnessed 90 percent reductions in high-tech theft losses (Littman 2003).[5] Lee and Whang's (2003: 24) case study estimates that Smart and Secure Tradelanes procedures reduce costs by reducing inventory and by reducing inspection time. They conclude, "These cost savings far exceed the costs of implementing electronic seals, the readers, and the other infrastructure investments." Firms qualifying for Technology Asset Protection Association (TAPA) certification may receive insurance discounts (Littman 2003).

Roles for Developing Supply Chain Security

The transformation to secure and efficient supply chain security requires *developing and providing policy direction* from both the public and private sectors. This requires leadership from government, domestically and internationally. At the same time, leadership within companies located throughout the supply chain is crucial to establishing priorities, developing multifunctional teams, and strengthening relationships and the flow of information from remote suppliers to customers.

Just as important as leadership within sectors, and perhaps even more so, will be the collaborative leadership of public and private officials working together to build security while eliminating unnecessary barriers and maximizing logistical efficiencies. Further, this must include not only the *Fortune* 500 companies but also smaller firms that are found throughout global supply chains. Similarly, it must include not just the industrial powers such as the G-8 countries (Canada, France, Germany, Italy, Japan, Russia, the UK, and U.S.), but must be *global in nature.*

Smaller companies are frustrated by the fact that only larger companies are likely to have a voice in the process, and that only larger companies will be able to afford the investment needed to stay in step with supply chain security. Some attention needs to be given to the needs of smaller companies, to make sure they have a voice and can remain both compliant and viable.

—Workshop on Supply Chain Security, Michigan State University, November 17, 2003

Assessing Supply Chain Security

International and domestic incidents over the last three years have emphasized the need for an integrated approach to supply chain security management. Just as a chain is no stronger than its weakest link, a supply chain is only as secure as its weakest link, which includes the suppliers, manufacturers, wholesalers, retailers, carriers, terminals, and governmental institutions that plan, manage, facilitate, and monitor the global movement of goods. The previous sections have described the key supply chain objectives and institutions. The challenge, however, is to determine the means to achieve supply chain security with the broad range of relationships, processes, and institutions involved.

While there has not been a systematic assessment of best practices related to supply chain security similar to that completed for typical supply chain management practices (Bowersox, Closs, and Stank 2000), a synthesis of the existing literature and management interviews can offer some insight regarding supply chain security best practices. The two assessments that make up this section provide a framework for evaluating supply chain security practices. The first one, "Supply Chain Security Assessment," takes the perspective of the firm and is appropriate for use by manufacturers, wholesalers, and retailers.[6] When assessing a firm's supply chain security capabilities, the evaluative characteristics consider the firm's capabilities from a number of perspectives. The first focuses on key firm relationships. The second focuses on the firm's refinement of existing processes to enhance security (personnel security, information technology, facility security, inventory security, transport equipment security, transportation tracking and visibility,

receiving, storage, shipping, management education, internal operations management, and supply chain education). The third focuses on the supply chain security incident management stages (planning, mitigation, detection, response, and recovery). For each perspective, the assessment describes a number of characteristics of the firm in increasing levels of sophistication. The second assessment, "Government, Carrier, and Terminal/Port Assessment" beginning on page 32, describes additional evaluative characteristics for key supply chain stakeholders including governmental institutions, carriers, and terminal/port operators.

In both types of assessment, three levels of security performance are described for each category. Basic (Level 1) refers to the minimum security practices that would be expected for organizational relationship management, process refinements, and incident planning processes. Typical (Level 2) refers to organizations that have extended reasonable security efforts. Advanced (Level 3) refers to the security practices that are characteristic of firms that have placed a very strong emphasis on enhancing supply chain security.

While the assessment is useful for benchmarking organizational security capabilities, it is not realistic that any firm can bring itself and its supply chain partners up to the advanced level overnight. As a part of the assessment process, the firm must determine the risks associated with its current performance level in each category. The relative cost/benefits related to each category's risk must then be evaluated to prioritize supply chain security initiatives. The resulting prioritized list should

then guide management actions to assure maximum utilization of resources while minimizing the impact to the supply chain.

While these levels characterize firms in increasing levels of sophistication, it should be noted that supply chain security is a journey, not a destination. While the Advanced column may represent sophisticated practices today, those same practices may be typical or even basic in the future. Just as institutions, technology, processes, and environments change, the practices must adapt as well. Nevertheless, these assessment frameworks provide some systematic direction for evaluating supply chain management security practices at this point in time.

The two assessments provide tools for firms and key supply chain stakeholders to benchmark their own practices, processes, and policies. Firms and stakeholders are encouraged to go through the assessments and "check off" the relevant categories as an initial step in assessing whether current practices fall in the basic, typical, or advanced level. Then the assessments can be viewed in the context of risk, utilized to gauge improvements, and ultimately used to develop metrics.

Supply Chain Security Assessment

Elements of the Supply Chain Security Assessment

Listed are the dimensions for evaluating firm supply chain security. For each dimension, the assessment tables list basic, typical, and advanced practices.

Relationships
Supplier
Government
Carrier
Terminal/Port Operator
Customer

Security Efforts within Existing Processes
Personnel Security
Information Security
Facility Security
Inventory Security
Transportation Security
Transportation Tracking and Visibility
Receiving Management
Storage Management
Shipping Management
Management Education
Internal Operations Management
Supply Chain Education

Incident Security Management
Planning Management
Mitigation Management
Detection Management
Response Management
Recovery Management

Relationships

Supplier Relationships
(Practices defining the nature of the firm's relationship with material suppliers)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
▫ Defines minimal supply chain security requirements in contracts	▫ Defines supply chain security requirements in contracts	▫ Includes specific supply chain security requirements in contracts as a condition for acceptance ▫ Mandates that suppliers adhere to established standards (e.g., Technology Asset Protection Association prior to bidding)
▫ Performs limited pre-screening of suppliers as a condition for bidding on contracts	▫ Considers security capabilities of potential suppliers as minor when proposals are evaluated	▫ Pre-screens potential suppliers with security capabilities as a major consideration
▫ Communicates defined security requirements for suppliers, but doesn't verify that practices are being implemented	▫ Enforces defined security requirements for suppliers	▫ Works collaboratively with suppliers to refine security requirements ▫ Replicates best practices and results among trading partners
▫ Allows suppliers to perform and report security self-assessments	▫ Performs announced inspections/assessments or validation by third party	▫ Performs unannounced inspections/assessments or validation by third party
▫ Has not established metrics for evaluating supply chain security performance	▫ Has established limited metrics for evaluating supply chain security performance and makes them available	▫ Has established comprehensive metrics for evaluating supply chain security performance and makes them available ▫ Regularly reviews and objectively grades suppliers regarding adherence to security standards

Government Relationships
(Practices defining the nature of the firm's relationship with local, regional, and national agencies)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
□ Informally tracks government regulations and implications for implementing supply chain security practices	□ Proactively tracks government regulations and implications for implementing supply chain security practices	□ Takes active role in initiatives to educate and exchange information with government officials responsible for enhancing supply chain security
□ Has informal procedures and processes to communicate security breaches to law enforcement	□ Has defined procedures and processes to communicate security breaches to local law enforcement	□ Has defined procedures and processes to systematically monitor and synthesize information regarding security breaches on a global basis
	□ Actively participates in associations and organizations offering seminars regarding supply chain security	□ Actively participates in cross-organizational initiatives to develop and influence governmental supply chain security policies
□ Has minimal awareness of global and government initiatives to enhance supply chain security initiatives such as WCO, ACI, C-TPAT, and CSI	□ Tracks public information regarding government initiatives to enhance supply chain security initiatives such as WCO, ACI, C-TPAT, and CSI	□ Takes active role in guiding and providing feedback for government initiatives to enhance supply chain security initiatives such as WCO, ACI, C-TPAT, and CSI
□ Avoids notifying government regarding vulnerabilities	□ Informally informs government regarding vulnerabilities	□ Has a defined process to inform government regarding known vulnerabilities
□ Does not adjust processes based on government security levels	□ Adjusts processes based on government security levels	□ Adjusts processes based on government security levels

Carrier Relationships
(Practices defining the nature of the firm's relationship with air, motor, pipeline, rail, and water carriers as well as with transportation service providers)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
☐ Requires carrier to meet minimum inspection standards	☐ Defines security checks and processes for carriers	☐ Involves carriers in setting standards and establishing security processes
☐ Gives limited consideration to security capabilities when selecting carriers	☐ Uses limited number of security capabilities when evaluating carriers	☐ Requires comprehensive security capabilities for carrier contracts ☐ Requires carriers to participate in "known shipper" programs such as offered in the European Union and the U.S.
☐ Takes no role in specifying driver requirements for carrier	☐ Defines general requirements for carrier drivers	☐ Defines specific requirements for carrier drivers
☐ Requires carriers to have appropriate licenses (e.g., hazardous materials)	☐ Regularly reviews license requirements (e.g., hazardous materials)	☐ Regularly reviews license requirements (e.g., hazardous materials)
☐ Allows carrier to perform and report security self-assessments	☐ Performs announced inspections/assessments	☐ Performs unannounced inspections/assessments
☐ Provides carrier drivers with minimal education regarding supply chain security issues	☐ Provides carrier drivers with education focusing primarily on asset security	☐ Provides carrier drivers with comprehensive education regarding their role in enhancing supply chain security
	☐ Requires background checks to be performed on carrier employees	☐ Requires thorough pre-hiring background and reference checks with regular re-checks to be performed on carrier employees
	☐ Requires that carriers have developed and documented response plans for likely security incidents	☐ Proactively tests carrier supply chain security capabilities and response plans

Terminal/Port Operator Relationships
(Practices defining the nature of the firm's relationship with private and public entities that operate air, ocean, and water terminals and ports)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
▢ Requires terminal operators to meet minimum inspection standards	▢ Defines security checks and processes for terminal operators	▢ Involves terminal operators in setting standards and establishing security processes
▢ Gives limited consideration to security capabilities when selecting terminal operators	▢ Uses a limited number of security capabilities when evaluating terminal operators	▢ Requires comprehensive security capabilities for terminal operator contracts
▢ Performs and reports security self-assessment	▢ Performs announced inspections/assessments	▢ Performs unannounced inspections/assessments
▢ Gives minimal consideration to port facility security capability when evaluating port bids	▢ Approves a Port Facility Security Plan and subsequent amendments	▢ Provides input to Port Facility Security Assessment and subsequent amendments
		▢ Provides regular feedback for terminal/port operator regarding supply chain security requirements and performance
		▢ Proactively tests terminal operators' supply chain security capabilities

Customer Relationships
(Practices defining the nature of the firm's relationship with customers)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
▢ No formal means for customers to provide input regarding supply chain security concerns	▢ Firm has established and publicized an individual or organization to receive customer supply chain security concerns	▢ Firm has established and publicized an individual or organization to synthesize information regarding customer supply chain security concerns and to develop implications
▢ Customer has a minimal consideration for supply chain security	▢ Customer recognizes supply chain security efforts as a cost of doing business	▢ Customer recognizes supply chain security capabilities as a competitive advantage
▢ Customer has expended minimal effort to guarantee continuous supply of critical components	▢ Customer has established initiatives to guarantee continuous supply of critical components	▢ Customer has defined plans to guarantee continuous supply of critical components

Security Efforts within Existing Processes

Personnel Security
(Practices that guide the firm's activities for selection and monitoring of personnel)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
▢ Has no "code of ethics" regarding supply chain security practices	▢ Has basic "code of ethics" regarding supply chain security practices	▢ Has comprehensive "code of ethics" regarding supply chain security practices
▢ Uses limited pre-hiring back-ground and reference checks with rare rechecks	▢ Uses thorough pre-hiring back-ground and reference checks with rare rechecks	▢ Uses thorough pre-hiring back-ground and reference checks with regular rechecks
▢ Uses no pre-hiring drug checks	▢ Uses pre-hiring drug checks as allowed by law	▢ Uses pre-hiring and random post-hiring drug checks as allowed by law
	▢ Trains personnel to observe for signs of employees who might be living beyond their means	▢ Trains personnel to observe for signs of employees who might respond to coercion

Information Security
(Practices that guide the firm's activities to guarantee information integrity, consistency, and timeliness)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
▢ Does not require pre-transmission of crew or cargo manifests	▢ Suggests suppliers and carriers transmit electronic crew and cargo manifests	▢ Contractually requires international carriers to transmit electronic crew and cargo manifests
▢ Firms in Level 1 supply chain partnerships engage in minimal, arm's-length relationships enabled typically by asynchronous, one-way data push communication mechanisms	▢ Firms in Level 2 supply chain partnerships are characterized by push and pull, asynchronous and synchronous, point-to-point client-server communication	▢ Firms in Level 3 supply chain strategic partnerships are characterized by peer-to-peer client-server communication
▢ Uses no backup power supply for operations and security systems	▢ Employs backup power supply for operations and security systems	▢ Employs backup power supply for operations and security systems
▢ Allows order and shipment documentation to be readily available to operations personnel	▢ Secures order and shipment documentation, but restraints can be overridden	▢ Makes available order and shipment documentation on a "need to know" basis only
▢ Allows order and shipment information to be available to a wide range of individuals involved in operations	▢ Controls access to order and shipment information by role and responsibility in the organization	▢ Controls access to order and shipment information on a "need to know" basis only

Facility Security
(Practices that enhance security of the firm's buildings and their surroundings)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
□ Relies on passive measures such as locked doors and fences for facility security	□ Relies on passive measures such as locked doors and gates and occasional human checking for facility security	□ Provides facility security using a combination of passive and active measures including fences, locks, video, and human inspections
□ Has minimal definition of secure areas	□ Has clear identification of secure areas	□ Has clear identification and monitoring of secure areas
□ Uses locking devices on external doors and windows	□ Uses locking devices on external and internal doors, windows, gates, and fences	□ Equips exterior doors and windows with alarms
□ Has no backup power for critical facility areas	□ Has backup power for key operational areas	□ Has backup power for key operational areas and high-value cargo areas
□ Has no established process for establishing and revising facility authorization cards or keys	□ Has defined process in place to establish and revise facility authorization cards and keys	□ Has defined process in place to establish facility authorization cards and keys with dynamic revisions for changes in personnel
□ Provides terminal security by fences	□ Provides terminal security through a combination of fences and video	□ Provides terminal security through a combination of fences, video, guards, and information technology tools (e.g., biometric personnel screening)
□ Uses no color coding for uniforms or ID tags to designate access privileges	□ Uses color coding for uniforms or ID tags to designate access privileges	□ Uses color coding for uniforms or ID tags to designate access privileges
□ Employs limited video monitoring of facilities and docks	□ Uses closed-circuit video monitoring of facilities and docks	□ Requires use of closed-circuit video monitoring of facilities, docks, and cargo

Inventory Security
(Practices that reduce the risk of inventory theft and diversion)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
▫ Production receipts are recorded based on deliveries to the warehouse	▫ Inventory receipts in the warehouse are matched with production quantities in the plant	▫ Positive matches are required for production and inventory receipt quantities
▫ Warehouse Management System does not track product movement by employee	▫ Warehouse Management System uses barcoding to track storage and retrieval of product by employee	▫ Warehouse Management System uses Radio Frequency (RFDC) to track storage and retrieval of product and movement by employee
▫ No separation of duties (e.g., single individual is responsible for receipts and withdrawals without oversight)	▫ Limited separation of duties or oversight	▫ Documented separation of duties and oversight minimize the opportunity for inventory theft or diversion

Transportation Security
(Practices that facilitate the reporting and recovery of goods lost or stolen in transit)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
▫ Has not defined security interfaces with carriers	▫ Has defined a single primary security contact with each contracted carrier	▫ Has established an Internet supply-chain-theft report that contains all the information to be reported to law enforcement
▫ Uses no standard procedures for seal control and usage	▫ Uses standard procedures for seal control and usage	▫ Uses standard procedures with regular audit procedures for seal control and usage
▫ Has established basic lost or stolen goods metrics	▫ Tracks lost or stolen goods by month	▫ Lost or stolen goods metrics demonstrate continuous improvement

Transportation Tracking and Visibility
(Practices that minimize risk of goods being lost, stolen, or diverted in transit)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
□ Achieves transportation visibility through phone and manual procedures	□ Makes real-time tracking capability a prerequisite for carrier contracts	□ Requires Supply Chain Event Management (SCEM) capability to proactively manage transport movements
□ Does not use real-time satellite tracking for containers	□ Uses satellite tracking of trucks and containers on a limited scale	□ Requires satellite tracking of trucks and containers as a condition of contract
□ Does not monitor transportation routing	□ Reviews and approves transport routes prior to movement	□ Requires approval by firm security of any deviation from approved transport routes
		□ Uses tracking and protocols to allow real-time notification of diversion to security and law enforcement
		□ Records and reports detected deviations from approved transport routes

Receiving Management
(Practices that minimize the risk of receipt of unwanted or unauthorized material)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
□ Has no standardized process to deter or prevent the introduction of unauthorized weapons, incendiary devices, explosives, or other contraband	□ Has defined and implemented standardized process to deter or prevent the introduction of unauthorized weapons, incendiary devices, explosives, and other contraband	□ Uses video and scanning technology to deter or prevent the introduction of unauthorized weapons, incendiary devices, explosives, and other contraband
□ Uses no verification of carrier personnel prior to allowing entry	□ Requires verification of carrier prior to allowing entry	□ Requires verification of carrier and driver prior to allowing entry
□ Uses no systematic checking of containers prior to release for re-use	□ Systematically checks containers prior to release for re-use	□ Systematically checks containers prior to release for re-use
□ Does not document receiving discrepancies	□ Documents receiving discrepancies using paper and photographs	□ Documents receiving discrepancies using electronic and video means
	□ Requires proper weighing, counting, and documenting of cargo/cargo equipment verified against manifest documents	□ Requires proper weighing, counting, and documenting of cargo/cargo equipment verified against manifest documents
	□ Separates employee parking from visitor parking	□ Controls access to employee parking by a gate/pass and/or decal system
□ Does not control private passenger vehicle parking	□ Restricts private passenger vehicle parking to designated areas	□ Prohibits private passenger vehicles from parking in cargo areas or immediately adjacent to cargo storage buildings

Storage Management
(Practices that minimize the risk of damage or theft of product in a storage facility)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
□ Does not segregate storage based on product type or destination	□ Segregates and marks international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, vault, caged, or otherwise fenced-in area	□ Segregates and marks international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, vault, caged, or otherwise fenced-in area
□ Co-locates break areas with storage or staging areas	□ Separates break areas from storage or staging areas	□ Separates break areas from storage and staging areas
	□ Maintains controlled access to high-risk areas	□ Requires signing in and out of high-risk areas

Shipping Management
(Practices that minimize the firm's risk of shipping unwanted material and having product stolen or damaged in transit)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
□ Has no standardized process defined for loading and sealing containers	□ Accepts the process of carrier or third party for loading and sealing containers	□ Defines a standard process for loading and sealing containers and completes periodic audits
□ Has no standardized monitoring of cargo loading process	□ Employs standardized monitoring of cargo loading process	□ Employs closed-circuit monitoring of cargo loading process with recordings to be maintained for a specified period
□ Has not established different policies for high-risk shipments	□ Has refined policies for handling high-risk shipments	□ Has extensive policies such as two drivers, use of GPS, escorted service, driver security training, and route varying for high-risk shipments
□ Has no formalized process for inspecting shipping container integrity prior to loading	□ Has defined process for inspecting shipping container integrity prior to loading □ Maintains proper storage of empty and full containers in a protected environment to prevent unauthorized access, including use of seals	□ Has defined process for inspecting shipping container integrity prior to loading with periodic unannounced audits □ Maintains proper storage of empty and full containers in a protected environment to prevent unauthorized access, including use of seals
□ Uses only physical seals for limiting access to containers	□ Tests electronic seals for monitoring access to containers	□ Contractually requires electronic seals for monitoring access to containers

Management Education
(Practices that provide firm management and employees with a broad understanding of the benefits and costs related to supply chain security)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
□ Supply chain security has limited top management visibility	□ Supply chain security is viewed as a "cost of doing business" by top management	□ Supply chain security is viewed as a competitive advantage by top management
□ Limited communication of security policies and standards to employees	□ Firm communicates security policies and standards to employees	□ Firm communicates security policies and standards to employees including consequences of non-compliance
□ No recognition of employees reporting suspicious activities	□ Public recognition of employees reporting suspicious activities	□ Public recognition and incentives provided for employees reporting suspicious activities

Internal Operations Management
(Practices that guide the firm in the establishment of policies to enhance internal security)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
▫ Gives responsibility for supply chain security to the security organization	▫ Delegates responsibility for supply chain security across a number of functional areas within the firm	▫ Centralizes responsibility for supply chain security management with a high-visibility cross-functional team
▫ Does not regularly review supply chain security procedures	▫ Reviews supply chain security procedures only on an ad hoc basis	▫ Reviews supply chain security procedures on a regular basis
▫ Posts minimal signage regarding security requirements for operations personnel	▫ Posts signage regarding security requirements for operations personnel	▫ Posts extensive signage regarding security requirements for operations personnel with references to centralized reporting
▫ Has no defined procedures and conditions for notifying Customs and other law enforcement agencies regarding shortages, overages, anomalies, or illegal activities	▫ Has defined procedures and conditions for notifying Customs and other law enforcement agencies regarding shortages, overages, anomalies, or illegal activities	▫ Has defined procedures and conditions for notifying Customs and other law enforcement agencies regarding shortages, overages, anomalies, or illegal activities
		▫ Maintains information to facilitate product tracking

Supply Chain Education
(Practices that develop a workforce knowledgeable in supply chain management and security)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
▫ Has not reviewed and documented overall supply chain with the goal of identifying potential security risk areas	▫ Has reviewed and documented overall supply chain with the goal of identifying potential security risk areas	▫ Has prepared educational material to provide guidelines for prioritizing efforts to minimize risks
▫ Has not identified supply chain security education alternatives	▫ Has identified supply chain security education initiatives, but does not have a plan for moving employees through the program	▫ Has identified supply chain security education initiatives and has a formal plan for moving employees through the program
▫ Does not conduct training drills and exercises	▫ Has begun to conduct training drills and training exercises	▫ Regularly conducts drills and training exercises
		▫ Extends its supply chain security training to its trading partners

Incident Security Management

Planning Management
**(Practices that guide the firm in identifying alternative sources and flows
if an incident were to deactivate a key supplier or carrier)**

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
☐ Has no planning process to identify impact of key suppliers	☐ Has established alternative material sources in the case of supply chain disruptions	☐ Works with suppliers to establish alternative source as part of contracting process
☐ Has no planning process to identify the impact of interruptions on major lanes	☐ Has established alternative carriers for use in the case of supply chain disruptions on major lanes	☐ Works with carriers to establish alternative providers on major lanes
☐ Is developing framework for defining relative supply chain risk by country	☐ Has defined framework and is rating countries on their relative supply chain risk	☐ Has prioritized countries regarding relative risk and has established initiatives to reduce the level of risk
	☐ Has established protocol with appropriate public and private sector partners	☐ Has established protocol and conducted exercises with appropriate public and private sector partners

Mitigation Management
**(Practices that guide the firm's efforts to reduce the risk that those incidents
would significantly inhibit a firm's ability to continue operations)**

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
☐ Has no comprehensive view or statement regarding its efforts to mitigate the risk of supply chain security initiatives	☐ Has a comprehensive view regarding its efforts to mitigate the risk of supply chain security initiatives	☐ Has a comprehensive view and statement regarding its efforts to mitigate the risk of supply chain security initiatives
	☐ Has established a communication system for critical incident management	☐ Employs redundant communications system for critical incident management
	☐ Has established protocol with appropriate public and private sector partners	☐ Has established protocol and conducted exercises with appropriate public and private sector partners

Detection Management
(Practices that guide the firm in the deployment and application of detection equipment)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
☐ Has no defined procedures for recognizing and recording security incidents	☐ Has defined procedures for recognizing and recording security incidents	☐ Has defined procedures for recognizing and recording security incidents and has established guidelines regarding appropriate responses
	☐ Has established protocol with appropriate public and private sector partners	☐ Has established protocol and conducted exercises with appropriate public and private sector partners

Response Management
(Practices that define how a firm designs the organizational response to an incident)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
☐ Has no defined plans to respond to supply chain security incidents	☐ Attempts to have defined procedures to respond to supply chain security incidents	☐ Has defined and practiced "crisis management" procedures for responding to supply chain security incidents
	☐ Has established protocol with appropriate public and private sector partners	☐ Has established protocol and conducted exercises with appropriate public and private sector partners

Recovery Management
(Practices that define the firm's anticipatory establishment of plans for incident recovery)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
☐ Has no documented recovery plans for supply chain security incident	☐ Has documented plans for responding to a supply chain security incident	☐ Has documented plans for responding to a supply chain security incident and has a defined process to reinstate operations
	☐ Has established protocol with appropriate public and private sector partners	☐ Has established protocol and conducted exercises with appropriate public and private sector partners

Government, Carrier, and Terminal/Port Assessment

Elements of Government, Carrier, And Terminal/Port Assessment

Listed are the dimensions that supply chain partners, including government, carriers, and terminal/port operations, should use in evaluating their security. For each dimension, the assessment tables list basic, typical, and advanced practices.

Government
(Practices that facilitate local, regional, and national government ability to both reduce the risk and respond to a security incident)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
□ Allows each response unit (i.e., Police, Fire, and Public Health) and municipality to develop its own supply chain security plans and responses	□ Facilitates integrated responses across municipalities but not across response units	□ Facilitates integrated planning and responses across municipalities and across response units
□ Participates in minimal joint government-industry initiatives to plan and test security incident response capabilities	□ Participates in joint government-industry initiatives to plan security incident response	□ Participates in joint government-industry initiatives to plan and test security incident response capability
□ Does not have any standardized process for evaluating security risk	□ Develops and maintains a standardized process for evaluating security risk	□ Develops and maintains a standardized process for evaluating security risk and regularly reports metrics
□ Has no clear definition of governmental chain of responsibility for reporting supply chain security incidents	□ Has a defined governmental chain of responsibility for reporting supply chain security incidents	□ Has a defined and well-communicated governmental chain of responsibility for reporting supply chain security incidents
□ Has no common process for sharing and synthesizing supply chain security incidents	□ Has a common process for sharing supply chain security incidents	□ Has a common process for sharing and synthesizing supply chain security incidents
□ Does not understand its role in supply chain security with respect to freight	□ Understands the importance of secure supply chains but is not organized to provide an integrated response	□ Understands the importance of secure supply chains and is organized to provide an integrated response
	□ Defines, evaluates, and reports security levels based on established criteria	□ Develops written security agreements with other governments to apply a common methodology using transferable and consistent standards
		□ Facilitates trade for trusted and cooperative shippers, carriers, and firms

Carrier
(Practices that facilitate a carrier's ability to minimize the risk of and respond to a security incident)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
☐ Meets minimum inspection standards	☐ Defines security checks and processes for facilities and vehicles	☐ Involves key customers in setting standards and establishing security processes
☐ Does not have a formal process for measuring its supply chain security capabilities	☐ Defines and reports a limited number of security metrics	☐ Defines and reports a comprehensive number of security metrics
☐ Performs announced inspections/ assessments of facilities and equipment	☐ Performs unannounced inspections/assessments of facilities and equipment	☐ Proactively tests carrier supply chain security capabilities
☐ Provides carrier drivers with minimal education regarding supply chain security issues	☐ Provides carrier drivers with education focusing primarily on asset security	☐ Provides carrier drivers with comprehensive education regarding their role in enhancing supply chain security
☐ Allows customers to take no role in specifying driver requirements for carrier	☐ Allows customers to specify general requirements for carrier drivers	☐ Allows customers to define carrier driver requirements as an element of the contract
	☐ Requires that background checks be performed on carrier employees	☐ Requires thorough pre-hiring background and reference checks with regular re-checks to be performed on carrier employees
☐ Requires carriers to have appropriate licenses (e.g., hazardous materials)	☐ Regularly reviews license requirements (e.g., hazardous materials)	☐ Regularly reviews license requirements (e.g., hazardous materials)
☐ Has not established different policies for high-risk shipments	☐ Has refined policies for handling high-risk shipments	☐ Uses biometric personnel screening coupled with continued development of security measures (e.g., biometric ignition systems) for high-risk shipments
☐ Makes no use of technology for communicating with and tracking vehicles on road	☐ Uses two-way communication such as cell phones to communicate with drivers on road	☐ Uses two-way communication and satellites to communicate with and track vehicles while on road
☐ Has no documented response plans for supply chain incidents	☐ Has developed and documented response plans for every security incident	☐ Has extensive response plans for potential security incidents
☐ Does no testing of response plans for supply chain security incidents	☐ Performs announced testing of response plans for supply chain security incidents	☐ Performs unannounced testing and tabletop exercises of response plans for supply chain security incidents
		☐ Participates in known shipper programs such as offered in the European Union and the U.S.

Terminal/Port Operator
(Practices that facilitate a terminal/port operator's ability to minimize the risk of and respond to a security incident)

Basic (Level One)	Typical (Level Two)	Advanced (Level Three)
□ Has no Port Facility Security Plan in place	□ Has an established Port Facility Security Plan, but it is not regularly maintained	□ Has an established Port Facility Security Plan and regularly reviews it
□ Terminal operators meet minimum inspection standards	□ Terminal operators define security checks and processes for monitoring	□ Terminal operators set specific standards, establish security processes, and regularly report metrics
□ Performs announced inspections/assessments	□ Performs unannounced inspections/assessments	□ Proactively tests terminal operators' supply chain security capabilities
		□ Establishes critical incident protocol including joint exercises with key public and private sector agencies
□ Provides terminal security through the use of fences	□ Provides terminal security through a combination of fences and video	□ Provides terminal security through a combination of fences, video, guards, and information technology tools
□ Firms minimally consider the Port Facility Security Plan	□ Firms approve a Port Facility Security Plan and subsequent amendments	□ Allows customers to provide input into Port Facility Security Assessment and subsequent amendments
□ Does not plan or test port facility responses to supply chain security incidents	□ Has developed plans for port facility responses to supply chain security incidents	□ Plans and regularly tests port facility responses to supply chain security incidents

Recommendations for Action

The following four recommendations result from a synthesis of previous literature regarding supply chain security and the Supply Chain Workshop at Michigan State University. The recommendations focus on:

- **Recommendation One:** Leadership and visibility

- **Recommendation Two:** Greater public-private partnership, such as through a joint forum

- **Recommendation Three:** Promotion of additional research to enhance knowledge of supply chain security issues

- **Recommendation Four:** Dissemination of knowledge through education and training

Figure 3 illustrates the inter-relationship between the recommendations and the resulting impact.

The central theme of the recommendations is that strong leadership is necessary from a combined public-private partnership to raise awareness of the importance of supply chain security as a national priority and to promote initiatives to assure results. The partnership should facilitate and prioritize the research and dissemination of information regarding supply chain security issues, best practices, and performance measures.

Figure 3: Recommendations

Recommendation One

Leadership

Recommendation Two

Public-Private Sector Collaboration

Recommendation Three

Research

Recommendation Four

Education and Training

Resulting Impacts

- Transforming the Security Industry
- Information Sharing
- Best Practices and Metrics
- Research Priorities
- Education and Awareness
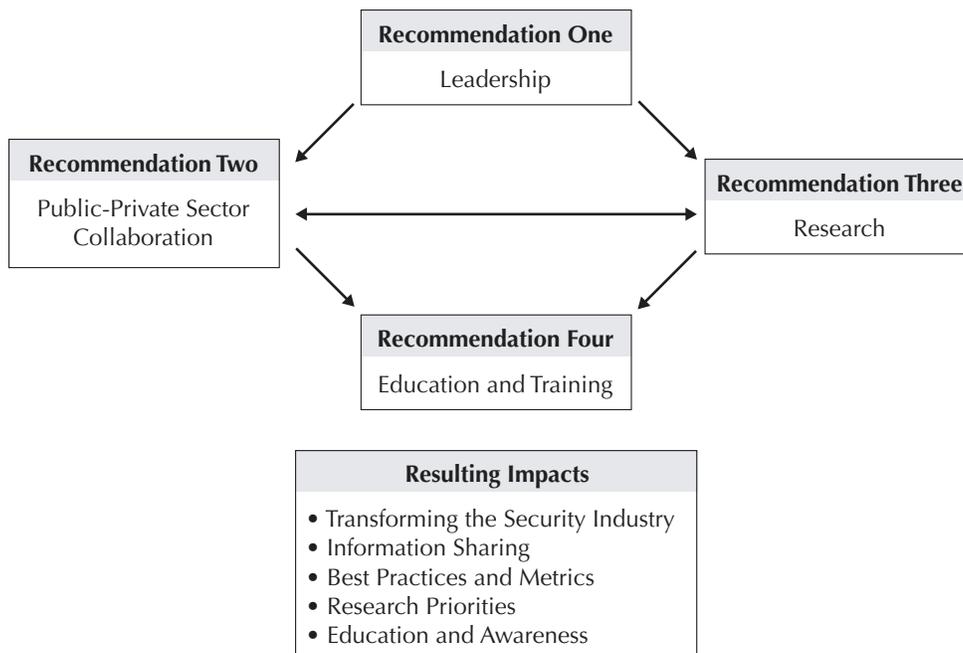
Recommendation One: Leadership. *Increase the awareness, visibility, and importance of supply chain security challenges and issues by fostering public-private sector collaboration and cooperation.*
There is need for a stronger, integrated message from both public and private sector leaders. Despite a number of important new initiatives increasing the security of the movement of people and goods, the sheer volume of global trade creates security challenges that demand the focused attention of government and industry leaders. This message must establish the link between the requirements for efficient movement to support a global econ-omy and the demands for security due to the war on terror. The result is that supply chain security is recognized across the board as a number one policy priority, and it must quickly and forcefully mobilize resources for lasting change.

There is a sense that the security industry as it operates within firms today is not engaged in the broader issues of supply chain security, but is still focused primarily on fixed asset security. There is a need to find a way to transform this industry, broadening its scope and role in the protection of supply chain processes, activities, and infrastructure, as well as firm assets.

This recommendation is similar to U.S. President John F. Kennedy's mandate regarding the space pro-gram in the early 1960s. A similarly unambiguous national commitment is needed, and it needs to be articulated by a broad spectrum of leaders so that everyone understands it as a fundamental necessity, not a product of politics or self-interest. Finally, the focus must transcend borders and be global in scope.

Recommendation Two: Public-Private Sector Collaboration. *Establish a forum that facilitates collaboration and joint action between government and industry to improve supply chain security risk assessment and identify best practices.*
There is a need for a government-industry forum to foster better information sharing among stakeholders that heretofore have not typically interacted. The group must be de-politicized, presenting supply chain security as an essential need for the liveli-hood and security of all. It must also be singularly focused on supply chain security and efficiency so that there is no dilution by other priorities.

The initial focus of the forum should be on two initiatives. First, the group should oversee develop-ment of a framework for assessing and prioritizing risk in the process of establishing supply chain security. The framework should include a focus on the critical activities and mission-critical elements. The phrase "mission-critical elements" is meant to include trade lanes, products, and infrastructure.

The second initiative should be to establish an effective platform for sharing information between government and industry, and within industries. Best practices, whether they are the best practices of a firm whose supply chain is secure or the best

Trust is needed if we are to develop good intelligence about vulnerabilities in the system and determine what needs to be done about them. Ideally, international governments and companies should be connecting the "best practices" of terror-ists with their likely consequences. But it is tremendously difficult for companies to openly acknowledge a deficiency or vulnerability, and thereby open themselves up to criticism from interest groups or regulators. In the absence of a shift in organiza-tional culture that encourages companies to identify what isn't working, compa-nies will continue to try to piece together a strategy for supply chain security internally, on their own. We need to find a way to elevate the internal function of identifying problems that put the company—and the supply chain—at risk.

—Workshop on Supply Chain Security, Michigan State University, November 17, 2003

practices of a terrorist seeking to disrupt it, must be communicated to all stakeholders in supply chain security. This recommendation calls for the establishment of a robust supply chain security intelligence collection system, one that facilitates information sharing and communication across the supply chain, and enables both government and industry to share essential information. This requires greater trust and a changed attitude toward the recognition of weaknesses within a company. Firms and the public sector must be willing to discuss weaknesses so that the combined partnership, represented by the government-industry forum, can propose common solutions that are both effective and efficient.

A key question that needs to be resolved is how the new entity would relate to the global community. What will be its relationship to the WCO, for example? It is clear that the forum should act in concert with national objectives. Yet, it is also clear that efforts to improve supply chain security must be global in nature if the supply chain is to be both efficient and secure.

Recommendation Three: Research. *Undertake research regarding the value and best practices related to supply chain security and disseminate the results.*
It is essential that the assessment of priorities, processes, practices, and the development of metrics occur in an environment that is objective and mutually respected by all stakeholders. This includes a combination of academic and governmental institutions, professional organizations, and private sector firms. The role of research is to facilitate key stakeholder collaboration, conduct research, and articulate the underlying value and necessity of maintaining supply chain security in language that speaks to all stakeholders. Relevant government-industry forums would facilitate research by identifying critical topics for investigation.

The advantages of broader, multidisciplinary research can be identified and disseminated to the institutional components of supply chains. For example, lessons learned in efforts such as the Business Anti-Smuggling Coalition, international drug enforcement, and anti-corruption initiatives can be applied to terrorist threats in today's supply chain environment. The packaging industry is

another important player in securing the supply chain. Access to and application of new technologies that can provide easier evidence of tampering, verification, and anti-counterfeit devices, for example, can greatly assist in achieving supply chain security through monitoring and detection.

There are three suggestions that require strong consideration when establishing the research agenda. First, the global nature of supply chains calls for a *global research network.* Such a network is much more likely to enlist the international support and cooperation necessary for common processes metrics, education, and innovation.

Second, there is a necessary intermediate step prior to the promotion of metrics and practices. The value of supply chain security must be illustrated through case studies that demonstrate the benefits and returns associated with successful risk mitigation. In the end, the case for supply chain security must be made in a *common language:* Its costs and its benefits must be conveyed in a wider, common context that both corporate and political leaders can easily understand and appreciate.

Third, research should explore the development of *assessment* tools to continuously validate and improve the process of implementing supply chain security measures. This suggestion addresses the ongoing work of maintaining supply chain security over time. It suggests that "tabletop" continuity tests should be conducted on an international scale to ensure that security measures remain current and effective.

The research, facilitation, and articulation that this entails must be carried out by entities that are mutually recognized as objective by both the public and private sectors. These entities must also be committed to objective metrics that can encompass the value of trade and its impact on the economy.

Recommendation Four: Education and Training. *Facilitate the development of education and training resources necessary to disseminate and implement best practices and approaches.*
This is the ultimate product of the previous three recommendations from the research and workshop: resources and programs to provide training to enhance supply chain security along with clear

metrics and best practices to guide managers and policy makers. The development of metrics is critical for creating a data-driven, reliable system that supports risk management models that allow for the development and valid identification of trusted partners.

Training and education regarding supply chain security should be incorporated into undergraduate, graduate, executive, and industry trade programs for a range of disciplines including business, security, public policy, and law. The education and training should include short modules and sessions that provide an overview to multiple-day programs, and semester classes that provide the information to guide assessment and implementation of supply chain security best practices. The content of education and awareness materials must be tailored to a wide range of audiences, from company CEOs to line workers, from government officials to international stakeholders.

Education and awareness are the essential goals of this recommendation; however, incentives for action will be important in engaging some audiences, such as "lower tier" suppliers and foreign partners. There is a general sense that incentives (e.g., accelerated cargo clearance associated with "fast lane" status, fewer inspections, etc.) have been and will be much more effective than penalties in bringing about the desired results.

Endnotes

1.   The report is based on a review of research and policy literature; dialogue with private and public sector leaders; a workshop on supply chain security involving 40 leaders from government, industry, and academia held at Michigan State University in November 2003; and the experience of leading academic programs in supply chain management and criminal justice/security at Michigan State University.

2.   The level of control of imports and exports varies with the movement of certain technologies tightly controlled.

3.   The AMR applied to sea cargo. The Advance Electronic Presentation of Cargo Information encompasses ocean, air, rail, and truck. Similar requirements were imposed by Israel in November 2003 and will soon be enacted in India for ocean and air shipments.

4.   "The Poka-Yoke system involves designing the process such that if some deviations to perfection happen in the production process, they could be identified right away and automatically corrected to prevent defects from recurring" (Lee and Whang 2003:8).

5.   Littman (2003) notes that successful efforts to reduce high-tech theft during the 1990s combined traditional security measures (guns, guards, and gates) with new technologically based steps including electronic tracking, alarm and access control, GPS systems, biometrically controlled ignition systems, etc.

6.   It should be noted that many aspects of the "Supply Chain Security Assessment" pertain to all stakeholders, but to differing degrees.

Bibliography

Bernasek, A. (2002). The friction economy: American businesses just got the bill for the terrorists attacks: $151 billion a year. *Fortune,* 145, 4: 104–110.

Bowersox, D. J., D. J. Closs, and T. P. Stank (2000). *21st Century Logistics: Making Supply Chain Integration a Reality* (Chicago: Council of Logistics Management).

Damas, P. (2002). Cutting red tape in cross-border trade. *American Shipper,* 44, 8: 14, 16–17.

Damas, P. (2001). Supply chains at war. *American Shipper,* (Nov.) 17–18.

Gillis, C. (2003). End-to-end customs control. *American Shipper,* 45, 3: 6–8, 10, 12.

Gillis, C. (2002). Customs agencies turn attention to exports. *American Shipper,* 44, 8: 8–10, 12–13.

Hannon, D. (2002). High-tech security becomes top priority in supply chain. *Purchasing,* 131, 11 (June 20): 39, 41.

Helferich, O. K. and R. L. Cook (2003). *Securing the Supply Chain* (Chicago: Council of Logistics Management).

Hickey, K. (2003). One strong chain. *Traffic World*, 267, 21 (May 26): 18–19.

Lee, H. and S. Whang. (2003). Higher supply chain security with lower cost: Lessons from total quality management. Graduate School of Business, Stanford University. 1–28.

Littman, J. (2003). Thwarting the perfect crime. *Electronic Business,* 29, 4 (April 1): 50–54.

Russell, D. M. and J. P. Saldanha. (2003). Five tenets of security-aware logistics and supply chain operation. *Transportation Journal,* 42, 4: 44–54.

ABOUT THE AUTHORS

David J. Closs is the John H. McConnell Chaired Professor of Business Administration in the Department of Marketing and Supply Chain Management at Michigan State University. He has been extensively involved in the development and application of computer models and information systems for supply chain operations and planning. Dr. Closs has worked with over 100 of the *Fortune* 500 corporations in areas involving logistics strategy and systems. In addition, he actively participates in logistics executive development seminars and has presented sessions in North America, South America, Asia, Australia, and Eastern Europe.

His primary research interests include logistics strategy, logistics information systems, and logistics planning techniques. He was one of the principal researchers guiding two studies investigating domestic and global logistics and supply chain best practices.

Dr. Closs has authored and co-authored numerous articles and made presentations regarding world-class logistics capabilities and logistics information systems applications. He is a co-author of *Supply Chain Logistics Management; Logistical Management: The Integrated Supply Chain Perspective; 21st Century Logistics: Making Supply Chain Integration a Reality;* and *World Class Logistics: The Challenge of Managing Continuous Change*. In addition, he has published papers in the *Journal of Business Logistics; International Journal of Physical Distribution and Logistics Management; International Journal of Logistics Management; Supply Chain Management Review;* and *International Marketing Management*

Dr. Closs received his Bachelor of Science, Master of Business Administration, and Doctor of Philosophy from Michigan State University.

Edmund F. McGarrell is Director and Professor of the School of Criminal Justice at Michigan State University. He also serves as Co-Executive Director of the Global Community Security Institute at Michigan State University (MSU). The Institute serves as an umbrella for MSU's homeland security initiatives that build on the university's particular strengths in interdisciplinary research, public-private partnerships, and online education tools.

In addition to homeland security, Professor McGarrell's research interests are in the area of communities and crime. He is the principal investigator of an initiative sponsored by the National Institute of Justice whereby the School of Criminal Justice is providing training, technical assistance, and research in support of Project Safe Neighborhoods (PSN). PSN is a major Department of Justice program intended to reduce firearms violence in the United States. McGarrell has conducted several long-term research projects including an experiment on the use of restorative justice conferences as an alternative response to juvenile crime and a strategic problem solving initiative to reduce homicide and firearms violence.

McGarrell's research has been funded by the National Institute of Justice, Office of Juvenile Justice and Delinquency Prevention, private foundations, industry, and state and local agencies. He is the author of *Juvenile Correctional Reform* and *Returning Justice to the Community: The Indianapolis Restorative Justice Experiment,* and co-editor of *Community Corrections* and *Community Policing in a Rural Setting*. His articles have appeared in a number of journals including *American Behavioral Scientist*, *Crime and Delinquency, Criminology and Public Policy*, *Journal of Research in Crime and Delinquency, International Journal of Comparative and Applied Criminal Justice, Justice Quarterly*, *Justice Research and Policy*, as well as reports by the Office of Juvenile Justice and Delinquency Prevention and the National Institute of Justice.

McGarrell previously was a faculty member at Indiana University, where he served as chair of the Department of Criminal Justice, and at Washington State University at Spokane. He previously served as director of the Crime Control Policy Center at the Indianapolis-based Hudson Institute, as co-director of the Washington State Institute for Community Oriented Policing, and was a visiting fellow at the National Center for Juvenile Justice.

McGarrell received his Bachelor of Arts degree from Mansfield University and and his Masters of Arts and Doctor of Philosophy from the School of Criminal Justice, University at Albany, State University of New York.

K E Y   C O N T A C T   I N F O R M A T I O N

To contact the authors:

David J. Closs
John H. McConnell Chaired Professor of Business Administration
Department of Marketing and Supply Chain Management
Eli Broad College of Business
N370 Business College Complex
Michigan State University
East Lansing, MI 48824
(517) 353-6381

e-mail: closs@bus.msu.edu

Edmund F. McGarrell
Director and Professor
School of Criminal Justice
Michigan State University
560 Baker Hall
East Lansing, MI 48824
(517) 355-2192
fax: (517) 432-1787

e-mail: mcgarrel@msu.edu

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
Steven I. Gordon

Privacy Strategies for Electronic Government (January 2001)

Janine S. Hiller
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
William Eimicke

State Web Portals: Delivering and Financing E-Service (January 2002)

Diana Burley Gant
Jon P. Gant
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
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
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
Michael Latham

Digitally Integrating the Government Supply Chain: E-Procurement, E-Finance, and E-Logistics (February 2003)

Jacques S. Gansler
William Lucyshyn
Kimberly M. Ross

Using Technology to Increase Citizen Participation in Government: The Use of Models and Simulation (April 2003)

John O'Looney

Services Acquisition for America's Navy: Charting a New Course for SeaPort (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

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
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
Fred Thompson

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
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
James Perry

The Procurement Partnership Model: Moving to a Team-Based Approach (February 2003)

Kathryn G. Denhardt

Moving Toward Market-Based Government: The Changing Role of Government as the Provider (June 2003)

Jacques S. Gansler

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

Alasdair Roberts

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
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
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
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
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
Trueman R. Tremble, Jr.

Human Capital Reform: 21st Century Requirements for the United States Agency for International Development (March 2003)

Anthony C. E. Quainton
Amanda M. Fulmer

Modernizing Human Resource Management in the Federal Government: The IRS Model (April 2003)

James R. Thompson
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 (November 2003)

Ray Blunt

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
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
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

Performance Management: A "Start Where You Are, Use What You Have" Guide (October 2002)

Chris Wye

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
Joseph S. Wholey

Performance Leadership: Eleven Better Practices That Can Ratchet Up Performance (April 2004)

Robert D. Behn

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
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
Barry Bozeman

NETWORKS, COLLABORATION, AND PARTNERSHIPS

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
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
Xavier de Souza Briggs

Collaboration and Performance Management in Network Settings: Lessons from Three Watershed Governance Efforts (April 2004)

Mark T. Imperial

TRANSFORMING ORGANIZATIONS

The Importance of Leadership: The Role of School Principals (September 1999)

Paul Teske
Mark Schneider

Leadership for Change: Case Studies in American Local Government (September 1999)

Robert B. Denhardt
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
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
Robert B. Denhardt

Transforming Government: Dan Goldin and the Remaking of NASA (March 2001)

W. Henry Lambright

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 Lambright

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
Fred Thompson

Managing the New Multipurpose, Multidiscipline University Research Centers: Institutional Innovation in the Academic Community (November 2003)

Barry Bozeman
P. Craig Boardman

SPECIAL REPORTS

Enhancing Security Throughout the Supply Chain
(April 2004)

David J. Closs
Edmund F. McGarrell

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
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

Managing for Results 2002
(Rowman & Littlefield Publishers, Inc., 2001)

Mark A. Abramson and John Kamensky, 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

* Available at bookstores, online booksellers, and from the publisher (www.rowmanlittlefield.com or 800-462-6420).

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.

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
website: www.businessofgovernment.org