RAND

INFRASTRUCTURE, SAFETY, AND ENVIRONMENT

RESEARCH BRIEF

Assessing Container Security

A Framework for Measuring Performance of the Global Supply Chain

RAND RESEARCH AREAS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND HOMELAND SECURITY
TRANSPORTATION AND INFRASTRUCTURE

Abstract

Since 9/11, several programs have been implemented to improve security of the global supply chain. In reviewing these programs, this study concludes that supply-chain efficiency and security are distinct but interconnected and recommends considering all aspects of supply-chain performance when assessing security measures. Also, programs to improve supply-chain security have focused largely on preventing and deterring terrorist attacks, with little focus on improving the supply chain's fault tolerance or resilience.

The global container supply chain moves cargo rapidly across seas and into ports throughout the world. A well-planned terrorist attack taking advantage of this system could occur anywhere, at any time. The significance of such an attack would be measured in terms of significant loss of life and billions of dollars of economic damages.

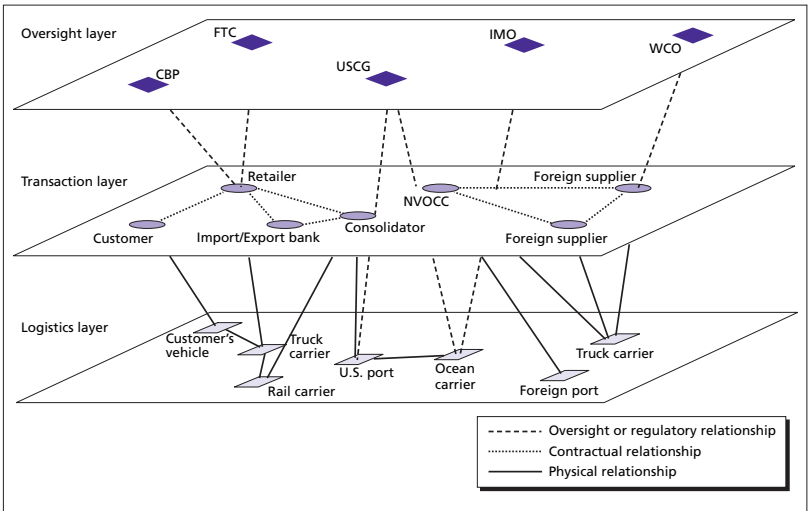
Traditionally, supply-chain security has focused on reducing shrinkage—the loss of cargo shipments through theft and misrouting. However, after 9/11, security has been redefined to include protection from terrorist attack. The response has been a proliferation of new security measures. But some fundamental questions remain: For all these efforts, is the system more or less secure? Will we know if these efforts are successful? How will success or failure be measured?

This RAND Corporation monograph presents a framework for addressing these questions by looking at the effects terrorist attacks might have and how the security measures themselves affect system performance.

What Does the Supply Chain Look Like?

The structure of the container shipping system would seem self-evident: It is a network of vessels, port facilities, rail cars, trucks, and containers that transport goods in discrete units around the earth. But that view pertains only to the physical components of a system that includes the cargo, information, and financial flows required for it to operate.

In fact, the supply chain can be viewed as three interdependent and interacting networks or layers, as shown in the figure: a physical logistics system for transporting goods; a transaction-based system that procures and distributes goods and that is driven



FTC = Federal Trade Commission; CBP = U.S. Customs and Border Protection; USCG = U.S. Coast Guard; IMO = International Maritime Organization; WCO = World Customs Organization; NVOCC = Non-vessel Operating Common Carrier

Corporate Headquarters
1776 Main Street
P.O. Box 2138
Santa Monica, California
90407-2138
TEL 310.393.0411
FAX 310.393.4818

primarily by information flows; and an oversight system that implements and enforces rules of behavior within and among the subsystems through standards, fines, and duties.

Examining the supply chain from these perspectives yields insights into the concerns of relevant stakeholders, the levers available to improve system performance, and the interactions among the layers that improve or detract from overall performance.

How Can Supply-Chain Performance Be Measured?

There are five inherent capabilities of supply-chain performance. **Efficiency**, the system's core capability, is measured in terms of speed, cost, and volume of shipments. **Shipment reliability** ensures that goods arrive within a specified delivery window with a minimum of loss from theft and accident. **Shipment transparency**, the ability to know what is being moved through the system, is needed to ensure that cargo is legitimately represented to authorities and is legal for transport. **Fault tolerance** relates to the system's ability to respond to disruptions and failures of isolated components without bringing the entire system to a grinding halt. Finally, **resilience** reflects the system's ability to return to normal operating conditions quickly after disruption of service.

While these capabilities, specifically efficiency and shipment transparency, are often seen as in direct conflict, we argue they are measured differently and may support or hinder one another, depending on the circumstances. Analyzing any program's efficiency and security implications requires considering the system under both normal and emergency operating conditions.

How Do Security Programs Affect Supply-Chain Performance?

Applying the layered capabilities framework to the analysis of current efforts to improve supply-chain security led us to two conclusions. First, **supply-chain efficiency and security are distinct but interconnected, meaning that all aspects of supply-chain performance must be considered when assessing security measures.**

For example, product theft is a business risk for all supply-chain users, and shippers and carriers have instituted security policies to combat it. But the benefits of the increased oversight and monitoring required to combat theft do not necessarily increase system efficiency. Actions that combat smuggling, likewise, have little effect on supply-chain efficiency; the smuggler's activities occur alongside normal business practices. Improving the two other system capabilities—fault tolerance and resilience—does not increase efficiency and, under normal operating conditions, might work against it. Both these properties imply a certain amount of spare capacity, particularly at port terminals but also on ships and at transshipment points. Spare capacity, under normal operating conditions, is a misallocation of resources.

The interconnected nature of supply-chain capabilities suggests that security measures that reduce efficiency could have unintended negative consequences because stakeholders will look for ways to compensate for or circumvent the security requirements.

Second, **initiatives to improve security have focused largely on preventing and deterring smuggling and terrorist attacks, with little focus on improving supply-chain fault tolerance or resilience.**

Our analysis shows that few security enhancement programs seek to ensure either fault tolerance or resilience. These capabilities are a function of both system design and the responses of participants in the oversight layer. In principle, it is in the best interests of a firm to plan for supply-chain failures. But at the logistical level, additional capacity is incredibly capital-intensive, and carrying it on a balance sheet makes little business sense.

For example, in 2002, the Ports of Los Angeles and Long Beach handled nearly three-quarters of all west-coast container traffic. This concentration is a vulnerability created by the drive for efficiency. Were both ports to close for security reasons, the other west-coast ports lack the needed infrastructure for absorbing all the traffic previously calling at Los Angeles and Long Beach. But while incentives for developing smaller ports would improve fault tolerance and resilience, they would also create redundancy and excess capacity that would reduce efficiency. Because these incentives do not exist and receive little attention from members of the transaction or logistic layers, public policy action is needed to provide the fault tolerance and resilience required.

Recommendations

These implications suggest three complementary paths for improving the supply chain's security while maintaining its efficiency. First, **the public sector should seek to bolster fault tolerance and resilience.** The motivation of the private sector to allocate resources to such efforts is subject to the market failures of providing public goods. Also, the government will be responsible for assessing security and for decisions to close ports.

Second, **security efforts should address vulnerabilities along supply-chain network trade lanes.** Efforts to improve security continue to focus on ports and facilities. But while the route over which cargo travels is vast and difficult to secure, doing so is essential to a comprehensive strategy to secure the supply chain.

Finally, **research and development should target new technologies for low-cost, high-volume remote sensing and scanning.** Current sensor technologies that detect weapons or illegal shipments are expensive and typically impose significant logistic system delays. New detection technologies for remote scanning of explosives and radiation would provide valuable capabilities to improve supply-chain security without diminishing efficiency. ■

This research brief describes work done for RAND Infrastructure, Safety, and Environment and documented in *Evaluating the Security of the Global Containerized Supply Chain*, by Henry H. Willis and David S. Ortiz, TR-214-RC (available at http://www.rand.org/publications/TR/TR214), 2004, 46 pp., $18.00, ISBN: 0-8330-3715-3. TR-214-RC is also available from RAND Distribution Services (phone: 310.451.7002; toll free 877.584.8642; or email: order@rand.org). The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.

RAND Offices Santa Monica • Washington • Pittsburgh • New York • Doha • Berlin • Cambridge • Leiden

RB-9095 (2005)