THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 10 NUMBER 1
AND HOMELAND SECURITY

JULY 2011
GLOBAL SUPPLY CHAIN

Contact: dhardy1@gmu.edu
703.993.8591

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

This month's issue of *The CIP Report* focuses on the various theories and solutions that pertain to managing and protecting the global supply chain.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

First, the President of the Council of Supply Chain Management Professionals (CSCMP) provides an overview of supply chain management (SCM) and its impact on the global economy. A Professor at George Mason University's School of Public Policy expands upon the volatility and risks in the global supply chain. Next, the links between critical infrastructure, the supply chain, and the economy in the United States is explained by two representatives from the Logistics Management Institute's (LMI) Infrastructure and Engineering Management Group and the Supply Chain Management Program. A Professor of National Security Affairs at the Center for Hemispheric Defense Studies at National Defense University illustrates the importance of protecting food in the global supply chain. A research project being conducted at Louisiana State University on the resource supply chain is described by three researchers working on the project. The Chairman of the Comité Européen de Normalisation (CEN) Workshop on "Container Security and Tracking Devices" and an independent consultant working on issues such as global Container Monitoring Service (CMS) discuss the role of real-time precise information from the operational supply chain. A Ph.D. researcher at the Faculty of Technology, Policy and Management at the Delft University of Technology analyzes risk management and paradoxical situations in modern supply chains. Finally, the Director of Maritime Security Issues at the U.S. Government Accountability Office (GAO) concludes the issue by examining supply chain security, specifically focusing on the Container Security Initiative (CSI).

This month's *Legal Insights* assesses threats to the global supply chain and their legal implications for businesses and organizations.

We would like to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

Supply Chain Management: The Driving Force behind the Global Economy

by Rick Blasgen, President and CEO,*
Council of Supply Chain Management Professionals (CSCMP)

The disciplines of logistics and supply chain management (SCM) have been around since the dawn of civilization. From the time that humans first appeared on Earth, they found it necessary to move things from one place to another, by foot or by hoof.

Fast-forward to the 21st century.

Think about breakfast this morning. The juice, coffee, cereal, fruit, and milk did not just appear. Nor did the toaster, refrigerator, or stove; not even the kitchen sink. Yet, these products are routinely available through the machinations of a dedicated group of logisticians and supply chain professionals and a complex, interconnected web known as the supply chain. Without them, people would still be milking their own cow.

Supply chain professionals order the product, move it, ship it, distribute it, and drive the coordination processes with marketing, sales, engineering, manufacturing, finance, and information technology. In short, they ensure that the goods consumers need are made available, wherever they are in the world. Also, supply chain managers move these products by the most efficient, cost-effective way possible, be it by truck, train, boat, or plane. We have come a long way since the days of the Pony Express.

Let us take a look at the evolution of SCM. Since the 1960s, it has evolved from "physical distribution" to "logistics" to "supply chain management"…from a humble, invisible corporate necessity to a critical component of commerce that has achieved global prominence on Wall Street and in boardrooms around the world. Supply chain management shed its dowdy image as a "cost center" in favor of the more glamorous one of "revenue generator." SCM has become a 21st century global superpower.

The Council of Supply Chain Management Professionals (CSCMP) was formed in 1963. Its original name was the National Council of Physical Distribution Management (NCPDM). The organization was created by a visionary group of managers, consultants, and educators who foretold the integration of transportation, warehousing, and inventory as the future of the discipline. Nearly 50 years later, it is apparent that CSCMP's founders were at the forefront of forecasting the future of the physical distribution field.

At CSCMP, we define SCM as that (discipline) which "encompasses the planning and management of all activities involved in sourcing and procurement, conversion, and all logistics management activities…."

Logistics is "that part of supply chain management that plans, implements, and controls the efficient, effective forward and reverse flows and storage of goods, and services…between the point of origin and the point of consumption in order to meet customers' requirements."

In simple terms, supply chain management and logistics connect supply to demand. We satisfy customers' needs at the lowest total delivered cost. SCM is also about transparency. Think about walking into a room and flicking on the light switch. The light comes on without thought. The electric company is not thanked when the lights work — but they are notified when the lights do not work.

It used to be the same thing for logisticians and supply chain managers. We did not get called unless something went wrong or was not delivered. We understood and accepted this, and kept the supply chain constantly moving, day and night, rain or shine.

But this, too, has evolved. As supply chain managers, our mission is vital. We deliver the products and services that our customers want and need to survive. Today,

(Continued on Page 3)

Management *(Cont. from 2)*

progressive SCM leaders are designing supply chain programs that include key participants in the process: suppliers on one end and customers on the other. They are taking a much more proactive approach in the design of their programs, thinking about how the supply chain can drive revenue while controlling costs.

The supply chain is a complex and sometimes fragile endeavor, dependent on a network of independent, yet interconnected, moving parts. It requires professional management. Every organization in the world is impacted by the supply chain because every organization has one. In today's world of expanding global trade and just-in-time sourcing, supply chain professionals need to be more resourceful than ever. The world is shrinking, and many organizations are as likely to source products from the other side of the world as from next door.

So what makes logistics and supply chain management work? A critical enabler is technology, which helps us move information faster and more accurately than ever before with just a click of a mouse or a single keystroke. Technology is key to helping us be more productive. But in the end, we still have to physically move product (efficiently) to get the job done…and done right.

We still have to put products in a factory-sealed case. We still have to stack it onto a pallet and load the pallet onto a truck. The product is then transported on the highways, railways, seaways, or skyways to its appointed destination. Once the product arrives, it must be taken off the truck (or railcar, ship, plane) and moved into a building. Sometimes it is stored again. Other times, it is loaded back onto another truck, where it travels down another road to another destination where it is eventually moved into a store. Then the product is put on a shelf where a consumer places it into his or her shopping cart. The enormous amount of physical movement required in logistics and SCM is important in keeping the global supply chain flowing.

Although technology has allowed supply chain managers to operate more efficiently and effectively, and has made supply chain "visibility" a reality, it is the people who make it all happen. The committed and dedicated logisticians who forecast demand, schedule production, select the proper transportation modes, connect with third party providers, and ultimately, satisfy customers, are the real heroes of the profession. At CSCMP, we are committed to advancing the profession and helping professionals succeed — in their companies and in their careers, through education and tools, research, networking, and a wide variety of outstanding SCM resources.

Global business leaders of today understand that effective supply chain management plays a critical role in the success of their organizations. The companies that will be the most successful in the 21st century recognize that, as supply chain managers move from the loading dock to the board room, they bring with them the key to corporate profitability.

About the Council of Supply Chain Management Professionals

Founded in 1963, CSCMP is the leading worldwide professional association dedicated to education, research, and the advancement of the supply chain management profession. With more than 8,500 members globally, representing business, government, and academia from 63 countries, CSCMP members are the leading practitioners and authorities in the fields of logistics and supply chain management. The organization provides individual and corporate members with the expertise and knowledge to help their companies create efficient, effective supply chains so they can successfully compete in the 21st century.

CSCMP also conducts hundreds of roundtables around the globe, making it easy for members to connect with their counterparts closer to home. 25,000 professionals attended CSCMP-sponsored events last year. In addition, CSCMP provides online and on-site professional educational opportunities to supply chain professionals near and far.

CSCMP's Annual Global Conference, October 2-5, 2011, will host over 3,000 supply chain professionals from around the world who will gather for educational information and networking

(Continued on Page 34)

Critical Infrastructure Protection: Volatility and Risks in the Global Supply Chain

by Irvin Varkonyi, Adjunct Professor,
George Mason University School of Public Policy and American Public University's Transportation and Logistics Management Program

The global supply chain, consisting of multiple activities, which cover the design, procurement, manufacturing, distribution, and consumption of goods, repeatedly demonstrates the co-existence of operational optimization with operational vulnerability. This was most recently and dramatically demonstrated in the aftermath of the tragic earthquake and tsunami which devastated the northern coastal region of Japan last March.

The Dilemma of the Global Supply Chain

The term "global supply chain" has grown in popular lexicon as technology, global trade agreements, and economic trends have coalesced over the past nearly two decades. An appropriate definition, among many, has been the movement of materials as they flow from their source to the end customer… including purchasing, manufacturing, warehousing, transportation, customer service, demand planning , supply planning …made up of the people, activities, information, and resources involved in moving a product from its supplier to customer (and back). These definitions have focused principally on operational optimization, but events have commanded stakeholders to recognize operational vulnerabilities. The tragic earthquake of March 13, 2011 off the northeastern coast of Japan and the devastating tsunami which followed have shattered the nation, with immense loss of life, property, and uncertainty of the future, not the least of which is the expected decades long impact of the nuclear reactors in Fukushima.

Japan has been a leader in manufacturing since the 1970s primarily due to the implementation of modern production methods. These methods have contributed to a robust economy and the position of the third largest economy in the world, behind the United States and China. Its innovations have been many, but among those with the most impact have been lean manufacturing and just-in-time (JIT) operations. The elimination of wasteful steps in operations, along with the integration of technology, enabled Japanese firms, especially automobile firms, to align quality with consumer demand and support a profitable enterprise. An intellectual basis of lean/JIT is an assumption of (relative) certainty, with respect to movement of goods and information.

Events of the past two decades have demonstrated that uncertainty is in fact becoming the norm in our world. Researchers at the University of Maryland Smith School of Business, in a study sponsored by the Council of Supply Chain Management Processionals, published findings this year "… of how companies survive and indeed prosper in a highly, volatile business environment. We argue that the nature of business today requires a new science of supply chain management — one based on rapid risk assessment and response. We call this new science X-Treme Supply Chain Management…the science of governing supply chains experiencing instabilities of unprecedented amplitude, frequency and duration."[1]

The Collision between Just-in-Time and Global Disruptions

The collision between lean/JIT and the extreme science of SCM have met with incredible force in Japan. There are similarities with other collisions:

- The 1995 earthquake in Taiwan, which disabled micro-chip makers' factories with an impact on U.S. computer manufacturers, nearly

(Continued on Page 5)

[1] Lisa Harrington, Sandor Boyson, and Thomas Corsi, *X-SCM: The New Science of X-treme Supply Chain Management*, Routleridge Press, (2011).

Volatility and Risks *(Cont. from 4)*

putting several companies out of business, including Apple Computers.

• The September 11, 2001 destruction of the World Trade Towers that exposed the vulnerability of organizations without adequate business continuity plans.

• The BP oil disaster in April 2010, which halted the important fishing and tourism industries on much of the Gulf Coast for a considerable period of time.

Regardless of the nature of disasters, be they natural disasters, intentional disasters, or unintentional industrial accidents, disruptions can be devastating. Short-term as well as long-term effects will vary based on a considerable number of variables.

The role played by Japan in global supply chains is critical, from automobile production to computers and high-tech items. Japan produces about 20 percent of the world's semi-conductors. This is actually a decrease from earlier years as firms sought to spread their risks. About a third of the world's memory chips are made in Japan but that figure has also been receding.

Can We Make Informed Decisions?

"The field of buying and shipping supplies has been transformed in the last decade or two. Globalization and technology have been the driving forces. Manufacturing is outsourced around the world, with each component made in locations chosen for expertise and low costs. So today's computer or Smartphone is, figuratively, a United Nations assembly of parts. That means supply lines are longer and far more complex than in the past."[2]

The impact, felt to be very difficult in the immediate aftermath of the earthquake, has become much more complex because of the high radiation levels that will essentially permanently affect production in a large part of the nation. Such an occurrence has been foreseen. A study in the March 2011 *Journal of Operations Management* issue stated:

"...sheds new light on a dilemma that has resurfaced amid global manufacturing and supply chain disruptions stemming from the recent earthquake and tsunami in Japan: while maximum efficiency may serve companies well when everything is flowing smoothly, firms with little or no resource slack are also highly vulnerable to any external shocks."[3]

The dilemma for global supply chains is where to find the sweet spot, or where efficiency is optimized but vulnerability is minimized. Risk management, an old profession focused on political and currency risk for the most part, must now deal with managing the risks of outsourcing, where metrics have not developed sufficient maturity. The field is gaining maturity as specialists develop algorithms which seek to guide organizations and quantify the risks of outsourcing in the global supply chain.

The publication, *Material Handling and Logisitcs*, considered the full landed cost of outsourcing in a recent article as the means to validate the positive return on investment of such a decision. While there are cost savings, i.e., labor, there are also increased costs, such as transportation, customs duties, etc. The unknown factor, the risk of disruptions, has likely been understated. "By re-defining the right set of response levers that will be activated in the event of a supply chain disruption, leading businesses are preparing themselves to manage supply chain contingencies based on long-term strategic priorities instead of scrambling to make hasty, ill informed decisions when the unthinkable occurs."[4]

Note a recent study by the Aberdeen Group, on supply chain visibility excellence, where a survey of global organizations confirmed the growing importance of visibility in the global supply chain based on demands for accuracy of movement and to provide early warning when disruptions have occurred.[5]

(Continued on Page 34)

[2] NY Times, (March 19, 2011).
[3] Sachin Modi and Saurabh Mishara, *Journal of Operations Research*, (March 2011), http://publications.mcgill.ca/reporter/2011/04/research-round-up-3/.
[4] Kelly Thomas, "Ten Thousand Miles of Risk Exposure," *Material Handling and Logistics*, (April 8, 2011).
[5] Bob Heaney, "Supply Chain Visibility Excellence," Aberdeen Group, (March 2011).

Critical Infrastructure and the Supply Chain

by Rich Skulte and Taylor Wilkerson,*
Logistics Management Institute (LMI)

The U.S. economy relies daily on the Nation's critical infrastructure to support the movement of goods, people, information, and money — the basic functions of a supply chain. Likewise, critical infrastructure is reliant on the availability of materials, people, and new technologies to maintain capabilities. No supply chain can operate efficiently without a modern and well-maintained supporting infrastructure, and no infrastructure can maintain its operational effectiveness without an efficient supply chain supporting it. The two work together to sustain our economy. Supply chain managers and infrastructure managers alike must be aware of the state of the infrastructure they use and the potential impacts to the economy should the infrastructure fail.

Critical infrastructure is a combination of organizations, facilities, networks, services, and assets; if disrupted or destroyed, the loss of these particular assets would have a serious impact on the health, safety, security, or economic well-being of a society, government, or business.

Twenty-seven days after the terrorist attacks of September 11, 2001, Executive Order (EO) 13228, relating to critical infrastructure protection, was signed. This EO established the Office of Homeland Security and the Homeland Security Council. In February 2003, the *National Strategy for Physical Infrastructure and Key Asset Protection* was released. This strategy finalized the formally recognized list of critical infrastructure.[1]

The critical infrastructure elements that most directly affect traditional supply chains are energy production, transportation infrastructure, and communications, as shown in Table 1. Additionally, there is a high degree of interdependence among critical infrastructure elements.

All elements of infrastructure must be upgraded and maintained to ensure proper operations. When repairs or upgrades are made to infrastructure, the supply chain delivers the materials needed to do the work. The supply chain can also be a source of innovation for infrastructure. Critical

(Continued on Page 7)

Energy	Transportation	Communications	Other
• Electrical power production, transmission, and distribution	• Railways, highways, shipping ports, and waterways • Airports and civilian aircraft • Postal and shipping services	• Telecommunications • Public and privately owned information systems • Hardware for Internet backbone and data storage systems	• Facilities that produce, use, store, or dispose of nuclear material • Critical facilities and other utilities • Agriculture, livestock, and systems for the provision of water and • Chemicals

Table 1: Critical infrastructure in the energy, transportation, and communications sectors most directly affects traditional supply chains

[1] J. Moteff and P. Parfomak, "Critical Infrastructure and Key Assets: Definition and Identification," Resources, Science, and Industry Division, Congressional Research Service, Library of Congress (2004).

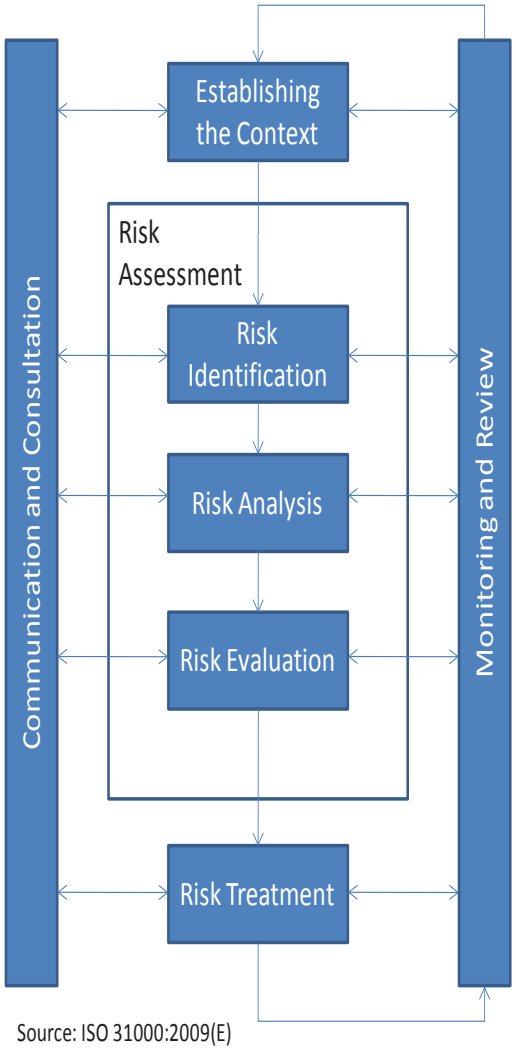
Critical Infrastructure *(Cont. from 6)*

infrastructure returns the favor to the supply chain by providing a steadfast foundation for responsive and reliable operations.

Supply chains across the economy rely on critical infrastructure; they need roads, railways, and airports to move goods. Supply chains also need effective communications systems to transmit information between trading partners. This allows efficient ordering and other communications. This process requires a reliable source of energy for producing and delivering items.

An example of the supply chain–centric impacts that infrastructure has on the economy can be seen in the interstate highway system. When the interstate highway system was built, the economy saw a 35 percent annual return on the investment in improved infrastructure. Even with a recent slowing of the rate of return, the interstate highway system has generated economic benefits far beyond its cost.[2]

The question then becomes: how to ensure that critical infrastructure continues to support efficient and resilient supply chains, and how to improve the supply chains that support critical infrastructure? The answer lies in the practice of supply chain risk management.



Source: ISO 31000:2009(E)

Figure 1: ISO 31000 risk management approach

Supply chain risk management (SCRM) is the practice of ensuring reliable operation of the supply chain in the face of potential disruptive events — also known as building a resilient supply chain. As we discuss how the supply chain and infrastructure can work better together, SCRM provides a useful lens.

ISO 31000 offers a proven process for managing risk, as shown in Figure 1. This approach is easily applied to managing risk in the supply chain for critical infrastructure. ISO 31000 highlights some key risk management concepts. First, risk management is a continuous process. Second, risk management starts with a strategic understanding of the operational context. Lastly, communication is a key component of effective risk management.

Managing risks to critical infrastructure begins with understanding the types of failures that can disrupt commercial supply chains. Since supply chains are heavily dependent on electrical power, transportation, and communications infrastructure, these are the elements that will be explored.

Electrical failure, more commonly referred to as power outages, occurs mainly due to storms or other natural events. However, it can also occur due to equipment failure, surges, or demand exceeding capacity. Power disruptions can cause production downtimes, loss of raw materials or products, or potential damage to equipment or processes. Outages can have high price tags, such as the estimated $2 billion in losses suffered in 2003 during the Northeast blackout by petroleum refineries and the

(Continued on Page 8)

[2] http://www.interstate50th.org/docs/techmemo2.pdf.

Critical Infrastructure *(Cont. from 7)*

chemical industry.[3] Fifty million people in the United States were impacted and rolling blackouts occurred for a week before power was fully restored.[4]

Transportation failure, or failure to deliver a material or product on time, may occur due to equipment failure, departure delays, traffic, overcrowding or understaffing of ports, and numerous other reasons. The infrastructure of transportation can involve many moving parts. Mechanical, process, or human failure can all contribute to a late delivery. Transportation failures result in late, postponed, or cancelled deliveries, which propagate down the supply chain and impact inventory, selection, lead-times, and ultimately, customer satisfaction and retention. In short — the cost of doing business increases.

Communication failures may occur due to power outages, software glitches, poor compatibility of new and legacy systems or versions, downtime due to network maintenance or lack of redundancy, etc. Since information technology control networks were initially designed for access, not security, they may also be vulnerable to hackers and other cyber threats. Communications are becoming increasingly sophisticated in being able to forecast supply and demand, but are reliant on, and leveraged with, previous communications. Therefore, a failure in communications may not only disrupt the flow of one or more supply chain nodes, but may also temporarily lower the accuracy of the predictive information that is being communicated. Communication failures may lead to low levels of reliability, late or incomplete orders, or poor visibility into customer demand. These failures may lead to costly contingencies, such as the need to carry excess inventory.

Since any single disruption of the supply chain can potentially have exponential or cascading effects, the reliability of the underlying infrastructure is critical. A model for critical infrastructure risk assessment is shown in Figure 2.

The ultimate focus of any SCRM process needs to be treating (reducing or eliminating) the risk in order to improve resilience. Effective treatments reduce one or more of the hazard, vulnerability, and consequence of the risk. Treatments must be tailored to the risk and the operating environment, but can include actions ranging from preparing an incident response plan to redesigning your supply chain to avoid high-risk locations or processes.

When addressing critical infrastructure, risk treatment becomes a more challenging topic. Since infrastructure is a shared public good, no single supply chain

(Continued on Page 31)

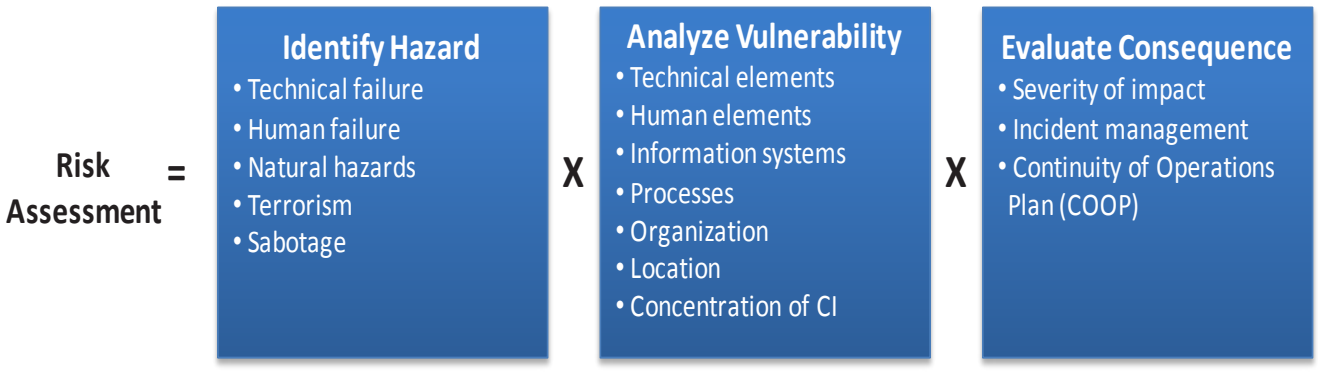


Figure 2: The risk to critical infrastructure is a product of the probability of a hazard, the degree of vulnerability of the critical infrastructure, and the severity of consequence[5]

[3] M. Merz and M. Hiete, "Management of Critical Infrastructure Disruptions in Industrial Supply Chains," International Disaster and Risk Conference, Davos, (2008).
[4] Electricity Consumers Resource Council, "The Economic Impacts of the August 2003 Blackout," (2004).
[5] Adapted from M. Merz and M. Hiete, "Management of Critical Infrastructure Disruptions in Industrial Supply Chains," International Disaster and Risk Conference, Davos, (2008).

Securing Global Supply Chains in an Age of Uncertainty: Focus on Food Safety

by Celina B. Realuyo,*
Assistant Professor of National Security Affairs, Center for Hemispheric Defense Studies,
National Defense University

The views expressed in this article are those of the author and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the U.S. government.

Since the fall of the Berlin Wall, we have been the beneficiaries of globalization — receiving goods, services, and information cheaper, faster, and better. More recently, with the global recession of 2008, we have witnessed the darker side of globalization with increased risks and uncertainty posed to all sectors of society around the world. An anemic economic recovery, burgeoning deficits, soaring commodity prices, natural disasters, and political unrest have led some to question the benefits of globalization and free market capitalism.

The first half of 2011 has been fraught with political and economic upheaval that has demonstrated how vulnerable we are in an interconnected world. From the devastating earthquake and tsunami in Japan, to the turmoil in the Middle East, we have witnessed how fragile global supply chains have become the "just-in-time" sourcing and delivery of key commodities, such as oil, and sophisticated high-tech components and finished products. The challenges of global supply chain management are not new; however, we now face an ever more complex world of fast breaking events that can have dire implications for supply chains and critical infrastructure throughout the world. There remains a need for international standards and vigilant oversight to safeguard global supply chains, especially when it comes to what we eat.

The Four Critical Elements of Global Supply Chain Management (The 4 M's)

Regardless of industry or sector, there are four critical elements of any global supply chain whose integrity must be preserved and protected at all cost:

1. **Material:** What is being moved through the supply chain? People, goods, commodities, services, data? Where are those materials coming from and where are they going?

2. **Manpower:** Who controls and staffs the supply chain? Who are the key enablers of that supply chain? Who is in control of these mechanisms or modes of conveyance?

(Continued on Page 10)

Food Safety *(Cont. from 9)*

3. Money: Who is funding or financing the supply chain? What business model is being used to generate revenue? Where is the financing originating from and where is it directed?

4. Mechanisms: What modes of conveyance are being used by the supply chain? Are people, goods, and services moving by land, air, sea, or cyberspace? How is the supply chain organized?

While each of these four critical elements of global supply chain management has their unique modalities, the security of each is paramount to safeguarding supply chains. Who is securing these elements? Global competition has led the private sector to identify and adopt the most efficient means of matching supply and demand for goods, services, and information and incorporate risk management mechanisms; however, international safety standards and government oversight still lag far behind.

Safeguarding Global Supply Chains: Focus on Fish Post-Fukushima

The earthquake and tsunami in Japan on March 11, 2011 was a human tragedy. The closing of ports and airports immediately after the disaster also disrupted global supply chains. Most global supply chain and risk managers focused on the impact on the transportation, energy, and electronics industries. When the sea near the Fukushima Dai-ichi nuclear plant showed elevated levels of radiation and cesium, the Japanese government began testing seafood for contamination almost daily since March 19, 2011.[1]

In the United States, the Food and Drug Administration (FDA) is the agency responsible for food imports to the United States. It increased surveillance of food products from Japan due to public health concerns of possible radiation and nuclear contamination of Japanese food exports. On March 22, 2011, the FDA issued an "Import Alert" that covered dairy products and fresh produce manufactured or from the affected prefectures in Japan.[2] Curiously, the Import Alert did not cover fish and seafood originating from Japan, but the FDA stated that "[o]ther food products from this area [of Japan], including seafood, although not subject to the import alert, will be diverted for testing by FDA before they can enter the food supply."[3] Since the FDA has been criticized for historically low import inspection rates of food products, the agency might expect critics to ask why the FDA did not include fish and seafood in the Import Alert for food imports from Japan from the start.

Representative Rosa DeLauro of Connecticut, leading Democrat on the House Subcommittee that oversees FDA spending, asked how the FDA could say with certainty that there is no threat to the U.S. food supply from Japanese radiation. She noted that the FDA is not always able to track where food production facilities are located in other countries and suffered from resource constraints.[4] In fact, the U.S. Government Accountability Office (GAO) released a report in May 2011, entitled *Seafood Safety: FDA Needs to Improve Oversight of Imported Seafood and Better Leverage Limited Resources,* that provided an unfavorable assessment of the FDA's efforts to inspect imported seafood.[5] These disconcerting shortcomings of the FDA call into question the government's ability to ensure the safety of our food supply from imported food.

To put things into perspective, according to the Congressional Research Service, seafood imported from Japan only makes up 2 percent of all seafood consumed in the United States. Some 15 percent of Japanese food exports are destined for the U.S. market, 75 percent of which consists of fish and Japanese

(Continued on Page 33)

[1] Reports are posted by Japan's Ministry of Health, Labor, and Welfare, "Information about 2011 Tohoku-Pacific Ocean Earthquake," http://mhlw.go.jp/english/topics/2011eq/index.html.

[2] U.S. Food and Drug Administration Import Alert, (March 22, 2011), http://www.accessdata.fda.gov/cms_ia/importalert_621.html.

[3] Renee Johnson, "Japan's 2011 Earthquake and Tsunami: Food and Agriculture Implications," Congressional Research Service, (April 13, 2011), 11.

[4] Msnbc.com, "FDA Halts Imports of Dairy, Produce from Japan; Seafood will Still be Sold but will be Screened First," http://www.msnbc.com/id/42215049/ns/health-food_safety/.

[5] Cochran: GAO Report Critical of FDA Inspections, *The Mississippi Business Journal*, (May 17, 2011), http://msbusiness.com/2011/05/cochran-gao-report-critical-of-fda-inspections/.

Disaster Supply Chain Structure and Management: A Preparedness and Response Model and Software

by Peter Kelle, Helmut Schneider, and Huizhi Yi,
Louisiana State University, Baton Rouge

Introduction and Literature

A critical component of emergency response is the resource supply chain. Absent sound analysis of how supply chains operate during disasters, organizations continue to underestimate disruption risk, and fail to take appropriate approaches to mitigate these risks proactively. The Federal Emergency Management Agency (see FEMA, 2009 and 2010) summarized the status of disaster supply in the United States. According to FEMA, the sourcing for disaster response is fragmented; the lack of integrated and coordinated supply management results supply delays on one hand and waste on the other hand. How could the pre-allocation of resources and the coordinated re-allocation be improved?

Louisiana State University (LSU) is considering the preparedness and response decision stages in disaster SCM. The first stage decision is the pre-positioning of different supplies (commodities like bottled water) to distribution centers before knowing any information on a specific disaster. The second stage decision is on the flow of the evacuees and reallocation of supplies after receiving more information on the particular disaster. In this model, the first planning stage costs include the holding cost of different goods at different distribution centers and the expected cost of the second stage decision, which is influenced by the first stage decision. The second stage response costs include transportation costs of evacuees and of resources, and the shortage or surplus costs of resources. The research is supported by a grant from the U.S. Department of Homeland Security (DHS).

The literature is rich in papers related to the disaster SCM area. Survey articles related to disaster supply chains include an operational research (OR) methodology survey by Altay and Green (2006), a risk mangement survey by Tang (2006), and an OR recovery planning survey by Osei-Bryson and Joseph (2009). Papers in the specifics of evacuation and sheltering planning include the papers of Sheral et al. (1991), Drager et al. (1992), Kongsomsaksakul et al. (2005), Liu et al. (2006), Yi and Ozdamar (2007), Sadatseresht et al. (2009), and Stepanov and Smith (2009).

Papers dealing with resource allocation and prepositioing include Bakuli and Smith (1966), Tufekci (1995), Lodre and Taskin (2009), Campbell and Jones (2010), Mete and Zabiski (2010), Taskin and Lodree (2010), and Rawls and Turnquist (2010). Application of stochastic programming is reported in Barbarosogcaronlu and Arda (2004) and in Liu et al. (2009).

These papers are all dealing separately with evacuation or with supply planning. The first paper that integrated evacuation and resource allocation was published by Li et al. (2010). LSU extends the integrated modeling approach with additional complexities in supply chain structure and decision alternatives.

The Two-Stage Stochastic Programming Model

In this model, the evacuee flow and the resource supply flow are connected. Based on disaster statistics, LSU developed scenarios which represent the potential locations and magnitude of the uncertain hurricane events that generate the evacuee flow to different shelters. The disaster supply structure consists of a complex supply network of government, charity, and business sources. The supplier side is hierarchical with three layers: local, State, and Federal distribution centers, where each layer can transport to all the lower layers. Figure 1 (Page 12) illustrates the evacuation and supply network.

The FEMA distribution network includes the layer of Federal depots (like Air Force Bases, Army Camps, and Incident Support Bases), and the layer of State depots (Regional

(Continued on Page 12)

Resource *(Cont. from 11)*

Staging Areas and Distribution Centers). The Non-Government Organizations (NGO) can be hierarchical (Red Cross) or ad hoc organizations (faith-based and community-based). The resources of private companies (grocery, home improvement, and pharmacy chains) are also considered.

We formulate the SCM problem as a two-stage stochastic program with recourse.

Stage 1: This stage occurs before hurricane season. The major goal is pre-positioning resources, and considering its effect on transportation and supply realized in Stage 2. The objective function is the total first stage cost of pre-positioning plus the cost of second stage evacuee transportation, resource distribution, inventory, and shortage cost for each disaster scenario, weighted by the probability of the scenario. Thus, in the first stage decision, the expected cost of the second stage is included. This is influenced by the first stage decision.

Stage 2: This stage occurs later in the hurricane season when a particular scenario is likely and the planning of evacuation and supply is done based on the information on this scenario. The cost and time of supply depends on the Stage 1 decision. The second stage is based on scenarios that pertain to the different possible locations and intensities of a hurricane hit. Each scenario generates a random percent of evacuees from different cities at or close to the expected hurricane.

In both stages, we include evacuee transportation and the resource balance equations connecting the three levels of the supply network and the shelter demands. The model allows resource shortage and surplus at shelters, therefore the feasibility is guaranteed under each scenario. The shortages indicate the demand that must be covered by additional orders as a specific hurricane hits. Additionally, the shelter capacities, resource capacities, and shipping capacities as constraints are considerd.

Software Product

The challenge of solving the proposed model primarily emanates from the large number of scenarios that are used to describe future disaster events. Commercial software such as Lingo, GAMS, or CPLEX solves only small-sized problems. Therefore, a new specific solution procedure is necessary.

The developed model is rewritten by separating the two stages of preparedness and response. The second-stage sub-problem is a linear program with continuous variables. Therefore, the recourse function is also continuous, convex, and at least piece-wise linear. As the number of second-stage scenarios is finite and the second-stage sub-problem for

(Continued on Page 30)

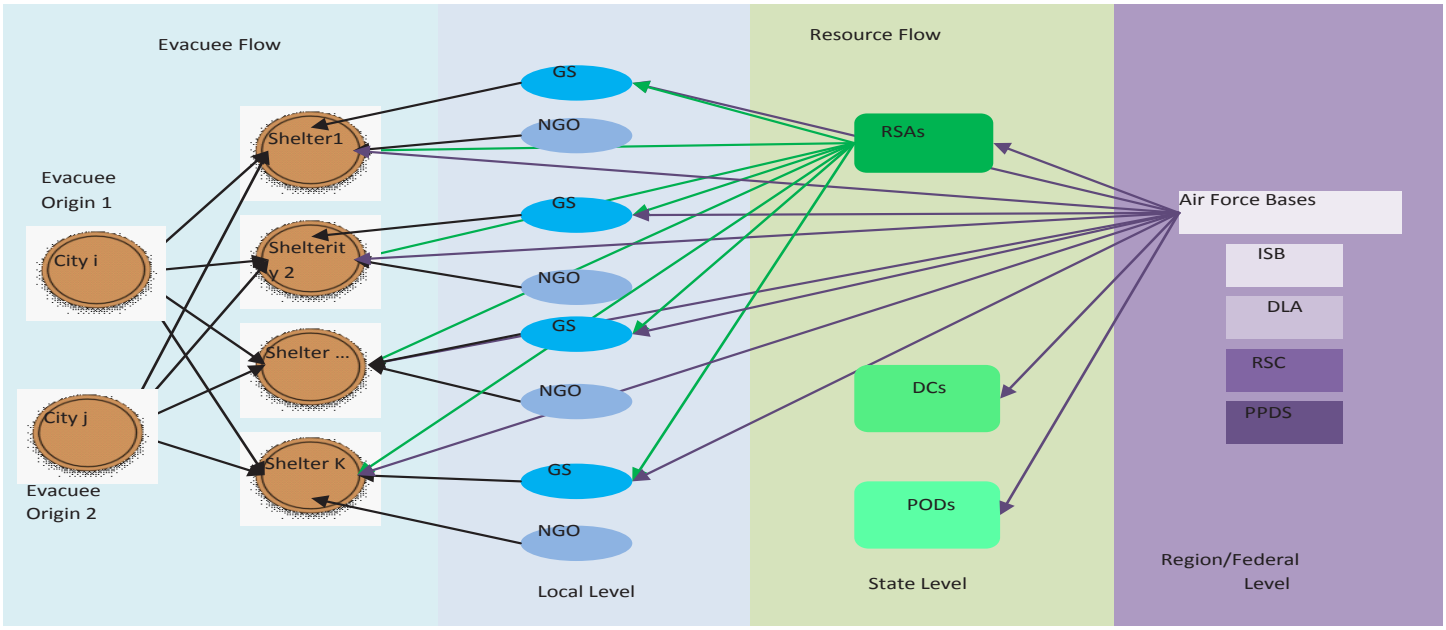


Figure 1: Disaster preparedness and response network

Understanding the Synergies between National Security and Business Value: The Role of Real-Time Precise Information from the Operational Supply Chain

by Joe McKinney and Arthur Radford*

Portions of this article were originally published as: "Real Financial Incentives Delivered: RFID Yields 'Precise Information,' Paving Way for Cost Elimination Opportunities," in "RFID News & Solutions," August 3, 2005.

What is it about Container Sensing Devices (CSDs), Real Financial Incentives Delivered (RFID), and other Auto-Identification (ID) technologies that are increasingly important to business operations? How can this same information enhance national and international security?

Introduction

CSDs and the other Auto-ID technologies provide the first opportunity for the efficient collection of "precise information" about the operations of an enterprise — each pallet, case, conveyance vehicle, unit, asset, component, associate, operator, supplier, customer, and in real or near real-time.

So what data are regulators around the globe now seeking? How will this data enhance national security for nations around the globe? Are there other regulatory uses for the data? And why would business operators collect and then feed such information to the regulatory agencies with the requirements? In the business context, these issues do not merit the commitment of time or financial investment until an enterprise has evidence of the value and the costs of its own response to the value of "precise information." If this information provides value to businesses, and the regulators are earning value from the same information, the serendipitous result is that regulatory agencies can tap into this same information for which the businesses have their own internal value proposition.

These results are currently being achieved in various global research and testing projects, two of which are known to the authors. These projects are sponsored by the European Union's FP7 Research grants: Project Integrity and Project SMART_CM Container Management. Both projects involve the collaboration of commercial, academic, and regulatory organizations.

In each of these projects, a substantial number (75-100 or more) of international container shipments have been monitored by Container Monitoring Devices (CMDs; also known as Container Security Devices or CSDs) from the time that the container is loaded and sealed until the time the container is unsealed and unloaded. During the entire journey, the device is reporting to its home monitoring system on a regularly scheduled basis as well as immediately in the case of an alert of some kind. The home system then parses the data into the message format required by the collaborative "data pool," known as "the Neutral Layer" in SMART_CM and as SICUS in Project INTEGRITY. These data pools are then accessed by the participating customs agencies, which can download and analyze the security data which has been collected.[1] If the agency wants to open the container for inspection, it can then communicate with the centralized data pool so that this legitimate regulatory inspection opening is recorded as a "safe opening" and not as a breach in security.[2]

These two projects have also demonstrated the principle of "interoperability," as the Neutral

(Continued on Page 14)

[1] Presently, security data is only in at the "door opening" status, but in the future will include other security condition indicators, such as presence of light, presence of carbon dioxide, and physical integrity of the container or trailers.

[2] The full results of these projects will be reported at the 4th European Conference ICT on ICT 4 Transport Logistics in Thessaloniki, Greece, (October 12-14, 2011).

Operational *(Cont. from 13)*

Layer has been able to exchange data with the SICUS database. This is important because a national customs agency may have its own "data pool" for various reasons, or perhaps several nations will have banded together to use one regional "data pool." Since it will be very inefficient for each container load, truckload, or rail wagon load to have its information reported into many data pools, these data pools must be able to inquire of each other for data which is required but is not resident in the customs agency's own data pool.[3]

Further questions to ask include, what is the motivation for the global shipping community stakeholders to participate in such a national security/regulatory system? Can Container Security Devices really serve the stakeholders as Container Monitoring Devices? And what cuts costs sufficiently to earn the investment required?

Digitization of Physical Product

Global positioning system or GPS based CSDs and the various versions of RFID make it possible, through digitization, to uniquely identify and represent electronically each object that must be handled in business operations. This process had already occurred for information (EDI) and for cash (EFT). Now, the entire set of supply chain flows — goods, cash, and data — can be both tracked and modeled at any level of detail found useful by the enterprise, bringing a level of precision to operations not formerly possible.

Additional forms of Auto-Identification Technology (AIT) extend the object information vector through the transportation process. This allows total information availability about items as well as their location and their condition at all stages in their shipping cycle, no matter the item's mode of shipment and transportation. Modern Auto ID systems include, for example, Real Time Locating Services (RTLS) and various types of cargo monitoring and condition sensing technologies such as the GlobalTrak® System developed by System Planning Corporation in Arlington, VA, and others that are available in the market today.

Since precise information, now efficiently obtainable through Auto ID, was not previously possible in a cost-effective manner, most management and business operators never needed to ask themselves the question: "can precise information improve the operations and the management of this business?"

Simply stated, the answer is "yes;" these results have been demonstrated in one form or another in nearly every analysis that the authors have performed. The logic is rather straight forward — CSDs, or more generically CMDs, provide data and information about a portion of normal corporate operations which has until now provided very little information about its

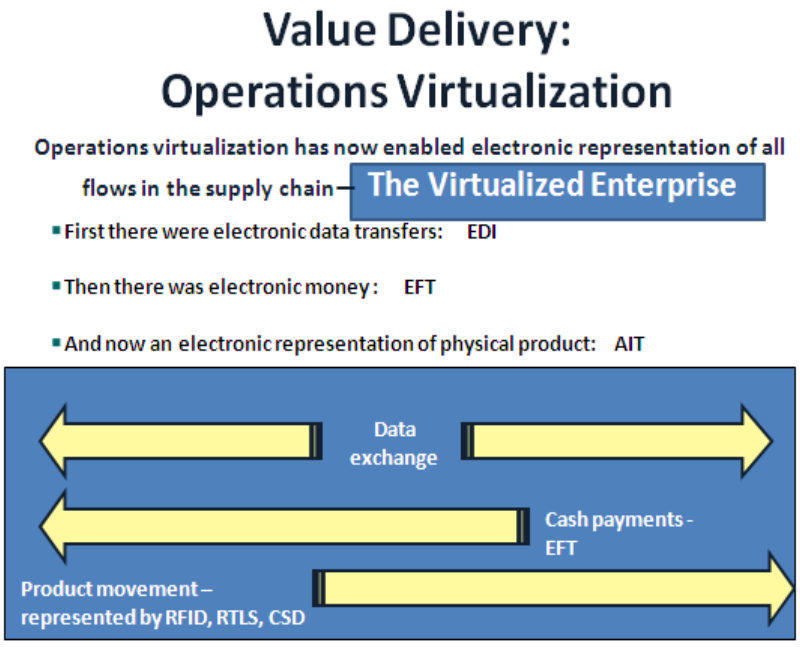


Figure 1

(Continued on Page 15)

[3] Fortunately this model of a global system architecture has already been proven by the consumer goods industry through the Global Data Synchronization Network (GDSN), established by the GS1 global organization.

Operational *(Cont. from 14)*

actual activities. For this reason, fully, 85 percent of the shrinkage[4] that occurs in the overall supply chain occurs while materials, components, or finished goods are in-transit from one location to another.

No longer must these expenses be considered as unmeasureable in that amorphous "cost of doing business" category. The availability of precise information directly from supply chain operations activities has been demonstrated to deliver, on average, supply chain operations cost savings of 3-5 percent and inventory investment savings of 7 percent and more. These savings combined reduce unit cost of goods sold by an average of 5 percent for the products that were analyzed, without impacting physical materials, production, or marketing costs.

Expense reductions were directly observed[5] in the following:

1. Reduced labor costs, derived by automating the actual tracking function, allowing the analysts to manage by exception. Thus, reducing the number of FTEs involved in monitoring each shipment.

2. Reduced shipment financing costs (interest) derived from reducing the duration of individual shipments.

3. Reduced shrinkage of all forms, including theft, damage, and delay.

4. Additional savings, which were indicated in these studies as potential for the future, but which were not observed directly:
a. Reduced insurance claims costs;
b. Reduced transaction processing costs.[6]

Observed inventory management cost savings are derived from the impact of using data and information to improve the consistency of and the measurability of actual in-transit supply chain operational performance. This enables lowering the statistical variances. Heretofore, this had been tolerated as "reality" because there was no observable real-time in-transit measurement of the actual events, delays, routings, and cargo environmental conditions. The combined impact of these variances had been increased safety stock, increased cycle stock, and the ever popular "just-in-case" stock.

The detailed data provided by the CSDs (or CMDs) has been observed to enable:

1. Reduced on-hand inventory, attributed to increased physical and logical visibility, which reduces the risks of shipping and the associated costs of:
a. Product
b. Financing
c. Handling

2. Reduced warehousing costs (less stock = less space).

3. Reduced inventory financing costs (visibility enables faster turns,

(Continued on Page 16)

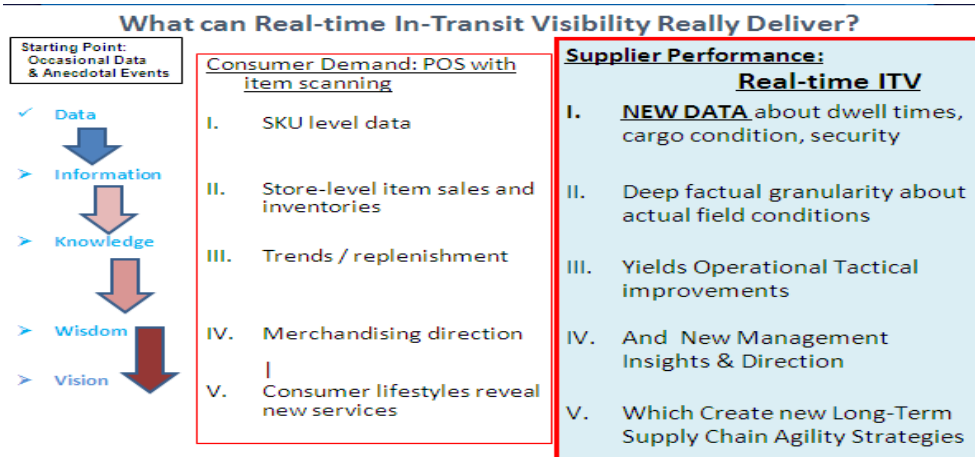


Figure 2

[4] Figure quoted by Dan Purtell, Senior Vice President, Supply Chain Solutions BSi, in a speech delivered to the "Global Supply Chain Summit-Securing Global Trade," Washington, DC, (April 5, 2011).

[5] These findings were observed in studies conducted in 2005-10 at IBM, Dow Chemicals, Transmed, Royal Foods, Target Stores, and Alicorp; the results at each company are confidential. Less rigorous analyses for JF Hillebrand, General Motors and Marks & Spencer's are the basis for Mr. Radford's Cost of Goods Sold (CGS) conclusions.

[6] This element should become more significant as users leverage the digitized information flow, but, transaction costs at the unit level are already so small as to be hard to measure, much less change overall COGS.

Operational *(Cont. from 15)*

lower holding times and associated costs).

Unquantified savings[7] (savings not yet quantified by real-world data) that should be cited are:

1. Brand protection and the incidence cost impacts: Mattel Toys, and recent outbreaks in Eurpoe.

2. Supply chain process improvements attributable to physical and logical visibility and the elimination of supply chain constraints that are in place without in-transit visibility.

3. Improved supplier performance by product sources and logistics service providers that a shipper will receive by leveraging in-transit physical and logical visibility, including the in-transit real-time shipment data that a CSD (CMD) senses and reports.

4. Reduced product damage costs derived from using the physical and logical data of shipments to identify both the causes and the occurrence locations of damages.

Conclusion

National security, for the United States and for other nations, can be greatly enhanced synergistically by encouraging all businesses to start real-time monitoring of their in-transit shipments. This newly available "precise information" about the status and the events that are occurring unseen by the stakeholders at either end of the shipment represents fertile ground for many operational and relational improvements in business, while also providing a few crucial pieces of data to regulators that are responsible for the security of all. The how, the why, and the technology choices can come later. ❖

Mr. Joseph McKinney is currently serving as the Chairman of the CEN (Comité Européen de Normalisation) Workshop on "Container Security and Tracking Devices." This position draws on his direct experience as the Vice President, Sales and Channel Management, the GlobalTrak®, and as a consultant with the Supply Chain Practice of CSC.

Mr. Arthur Radford led the development of the IBM Strategic Trade Lanes (STL) Container Monitoring Service (CMS) business and financial solution. He was recruited by Savi Networks LLC as Director of Client Services for their deployment of a global *CMS, successfully selling a number of service deployments. As an independent consultant, he has advised QinetiQ NA on developing its asset management solution and is working with EU and US based asset management and tracking service providers.*

Related References:

Barua, A., Mani, D., and Whinston, A. B., *Assessing the Financial Impacts of RFID Technologies on the Retail and Healthcare Sectors*, Center for Research in E-Commerce, Department of IROM, McCombs School of Business, University of Texas at Austin, (2006).

Kelepouris, T., Da Silva, S. B., and McFarlane, D. C., *Automatic ID Systems: Enablers for Track and Trace Performance*, in *Aerospace-ID Technologies WhitePaper Series*, Auto-ID Labs, Cambridge, UK, (2006).

Kelepouris, T., *A Data Model for Measuring the Economic Value of Auto-ID Generated Data*, in *Aerospace-ID Technologies White Paper Series*, AutoID Labs, Cambridge, UK, (2007).

Kelepouris, T., and McFarlane, D. C., *Determining the Value of Asset Location Information Systems in a Manufacturing Environment*, paper presented at the 19th Annual Conference of the Production and Operations Management Society, La Jolla, California, (2008, May 9-12).

Kelepouris, T., McFarlane, D. C., and Parlikad, A. K., *Developing a Model for Quantifying the Quality and Value of Tracking Information on Supply Chain Decisions*, paper presented at the International Conference on Information Quality, Boston, Massachusetts, (November 9-11, 2007).

Dr. Kelepouris's doctoral thesis at Cambridge University, entitled *The Value of Supply Chain Tracking Information*, covers the following:

a. An analytic model that describes

(Continued on Page 33)

[7] Additional analytical work performed by Mr. Radford while he was employed by IBM and then by SACI Networks support these observed, but at the time, non-quantifiable cost savings.

Risk Management and Paradoxical Situations in Modern Supply Chains

by Behzad Behdani,
Delft University of Technology, Faculty of Technology, Policy and Management

Several new trends in international trade, beginning in the 1990s and still part of the main paradigm in managing business, together with higher level of competition in the markets generate two inherently paradoxical situations in managing today's supply chains. First, two main factors put companies in a more risky position. These factors include higher number of risk sources in a supply chain and faster propagation of risk impact in the network. However, and paradoxically, the access to the resources needed to manage those risks has become much more limited. The outcome of this paradoxical situation is a growing vulnerability in supply chains and higher impact on the companies' performance. Indeed, running a smooth operation in supply chains and providing reliable service to the customers seem more challenging than ever before. Couple this fact with the highly competitive nature of business and growing expectation of customers, and we may find 21st century companies in a second-level paradoxical situation (see Figure 1).

More Risk Sources in Supply Chains

Compared with the traditional business, managers in firms must face more risk factors in their supply chains these days. Many of these new risk factors have originated from two influential features of business management in the 1990s: globalization and outsourcing.

As economies around the world have become increasingly global, the extended supply networks face many new types of risk, including natural disasters, political/social instability, cultural/communication inconsistency, exchange rate fluctuation, and local legislations. Traditionally, these risks were

(Continued on Page 18)

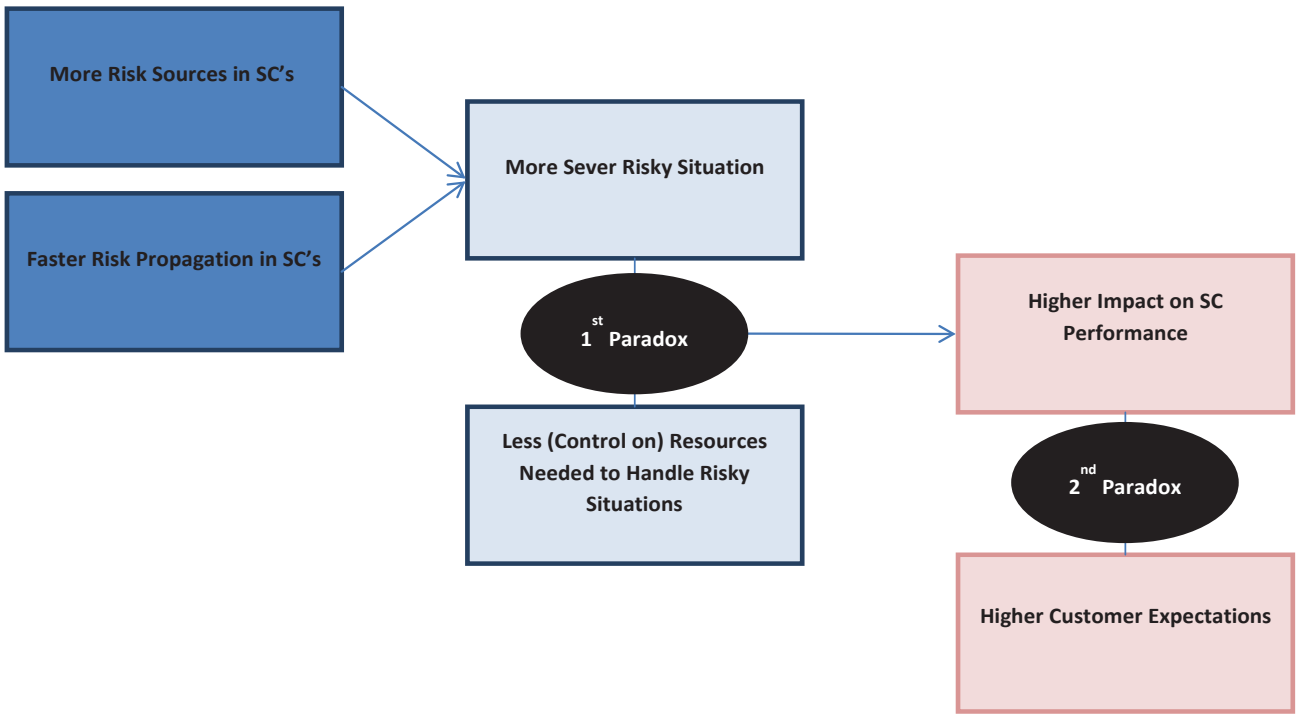


Figure 1: Two paradoxical situations in managing supply chains

Risk Management *(Cont. from 17)*

considered "country/region-specific." But, with significant change in attitude toward global trade and investment, they are not national or regional anymore. They can easily influence companies working miles from other regions and countries. For example, cultural differences and norms are blamed for increasing the rate of product recalls in recent years;[1] China's initial unresponsive and surreptitious approach is discussed as a key factor for the influence of SARS crisis on global supply chains;[2] and more recently, the terrifying pain of the Tōhoku earthquake and the destructive tsunami afterwards has been felt by many local Japanese plants and across many supply chains far from the center of the earthquake.[3]

Furthermore, more globalization in international business offers another significant challenge for companies around the world: they have to deal with longer lead-time (and consequently, higher uncertainty) in their global supply chains. This explains the critical role of transportation in global business. As an explicit consequence, another important class of risk might be highlighted in the risk profile of global companies: "transportation risk."[4,5]

Besides globalization, outsourcing has brought in several new risks for supply chains. Dependency on the quality of materials and services from an insourcer and the possibility of opportunistic behavior for participants with different and even conflicting goals are examples of these new risk factors.

The other risk factor that has become important due to the growing tendency towards outsourcing is the "intellectual property risk." With outsourcing and integration in the world economy, the intellectual properties of companies are increasingly at risk. Accordingly, protecting intellectual properties is a key concern in the modern business environment shifting towards knowledge-based economics. The insufficient laws in the judiciary systems of some host countries might intensify the issue.[6]

A recent study adds more information to the risks introduced by outsourcing to focal companies. This study shows that many businesses are ill-prepared for the time when the cooperation between the outsourcing and insourcing company will terminate. This transition to build new cooperation schemes with new partners may involve many challenges and risk factors for both the insourcer and outsourcer.[7]

Faster Risk Propagation in Supply Chains

In addition to new types of risks introduced by cost-efficiency trends in managing supply chains, companies must deal with another important and painful, fact: disruption in one specific part of a global supply chain can ripple down the chain much faster nowadays. This fast propagation of disruption effects in supply chains is chiefly due to lack of excess resources and redundancies across the system.

Traditionally, supply chains were designed with some redundancies in different segments. These buffers — whether in the form of excess stock, time, etc. — would help

(Continued on Page 19)

[1] Aleda V. Roth, Andy A. Tsay, Madeleine E. Pullman, and John V. Gray, "Unraveling the Food Supply Chain: Strategic Insights from China and the 2007 Recalls," *Journal of Supply Chain Management*, 44 (2008), 22.

[2] Wei-Jiat Tan and Peter Enderwick, "Managing Threats in the Global Era: The Impact and Response to SARS," *Thunderbird International Business Review*, 48 (2006), 515-536.

[3] Behzad Behdani, "Japanese Catastrophe and the Dark Side of Global Supply Chains," (2011), Next Generation Infrastructures website, http://www.nextgenerationinfrastructures.eu/index.php?pageID=5&itemID=564591.

[4] A 2008 survey by the consulting company PRTM found that companies consider on-time delivery of critical products as well as overall product/supply availability as major risks when globalizing their supply chain [Global Supply Chain Trends 2008-2010, Sixth Annual Survey by PRTM, 2008, http://www.prtm.com/strategicviewpointarticle.aspx?id=2392&langtype=1033].

[5] Another recent report of the practitioners' view on expected risk in their supply chains show that "many companies are encountering issues with global sourcing, including unreliable delivery (65 percent of respondents), longer lead times (61 percent) and poor quality (61 percent), with an additional 15 percent anticipating such problems within the next three years," [Karen Butner, "The Smarter Supply Chain of the Future," *Strategy and Leadership*, 38 (2010), 22].

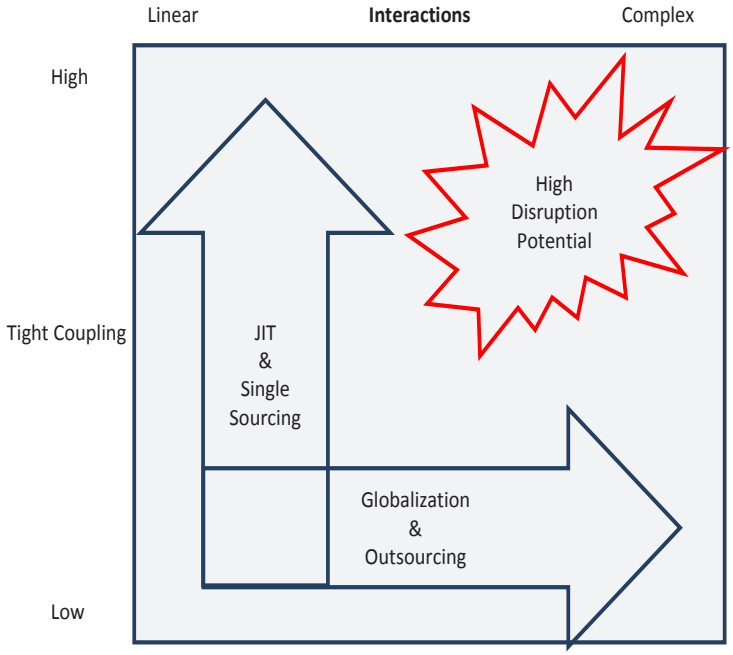
[6] "Doing Business in China: 850,000 Lawsuits in the Making," *The Economist*, (2008), http://www.economist.com/node/11023270.

[7] Klemen Kavcic and Mitja I. Tavcar, "Planning Successful Partnership in the Process of Outsourcing," *Kybernetes*, 37 (2008), 241.

Risk Management *(Cont. from 18)*

companies to better handle fluctuations in the daily business. Moreover, facing with breakage in their supply chains, they had extra time to plan for managing abnormal events. This is because the influences could be handled partly with some redundancies in the chain. However, hoping to eliminate all forms of wastes and buffers, many companies took some approaches like lean and just-in-time manufacturing. The potential gains of those philosophies in the stable business environment were huge. By holding fewer buffers, such as less stock and working with less suppliers, the operating costs of business were decreased considerably. Also, companies could benefit from the value of money savings by less investment, e.g., in the storage facilities. Nonetheless, along with these enormous benefits some pitfalls have emerged; working lean and a lack of buffer contribute to faster spread of risks in global supply chains. Facing a disruption, there are very limited buffers in different tiers of supply chains to bear the impacts. Accordingly, the adverse effects of initiating events spread quickly downstream of supply chains. Consequently, there is little time for the companies to find appropriate response solutions to handle those abnormalities.

Figure 2: NAT framework and business trends in managing supply chains



More Severe Risky Situation

Increasing the risk factors in supply chains on one hand and the rapid propagation of disruption impacts in supply network (because of high level of interdependencies and lack of buffer) on the other hand, put many companies in a challenging situation; they must work in a more risky and unsafe business environment.

Many studies have approved this increase in riskiness of the daily business of companies. Almost two thirds (65 percent) of about 3,000 executives surveyed in a 2006 McKinsey and Company Global Survey of Business Executives reported that their firm's supply chain risk had increased over the past five years (during the 2001-2006 period).[8] In a 2008 report, the situation was even worse since it claimed that 77 percent of respondents believe that the degree of risk their companies must face in the supply chain has increased in past five years.[9]

Another study by Lloyd's, in association with the Economist Intelligence Unit, shows that over a one-year period, one in five companies suffered significant damage from failure to manage risk and more than half experienced at least one near miss.[10]

The increasing exposure of supply chains to risks and disruptions is

(Continued on Page 20)

[8] "Understanding Supply Chain Risk: A McKinsey Global Survey," *The McKinsey Quarterly*, (2006), http://www.mckinseyquarterly.com/Understanding_supply_chain_risk_A_McKinsey_Global_Survey_1847.

[9] "Managing Global Supply Chains: McKinsey Global Survey Results," *The McKinsey Quarterly*, (2008), http://www.mckinseyquarterly.com/McKinsey_Global_Survey_Results_Managing_global_supply_chains_2179.

[10] "Taking Risk on Board" (2006), http://www.lloyds.com/Lloyds/Press-Centre/Press-Releases/2005/10/~/media/Lloyds/News/Press_releases/News%20Centre%20Gallery/2005/11/Takingriskonboard_pdf.ashx.

Risk Management *(Cont. from 19)*

also studied from many theoretical perspectives. One of these theories is the Normal Accident Theory (NAT). This theory argues that in the conditions of high "Interactive Complexity" and "Tight Coupling," the occurrence of accidents in the socio-technical systems is more likely or, as Charles Perrow describes, "normal."[11] A system is tightly coupled when there is little or no slack within the system and between different parts and functions and it is interactively complex when its sub-systems (actors or different functions) are connected and interact in many different (and unanticipated) ways. To avoid accidents, NAT suggests that firms must make the choices to either reduce their complexity or loosen coupling.

So, based on NAT, just-in-time production makes supply chains more vulnerable to disruptions due to the high level of "tight coupling." Consequently, to avoid "Normal Accidents" in a lean supply chain, the interactions must be necessarily less and the processes must be kept linear. Similarly, globalization and outsourcing increases the risk of exposure in supply chains due to the higher level of "interactiveness" in the system; supply chains are growing in size, more actors are involved, and many different functions in those companies must be aligned and coordinated. This will unavoidably increase the probability of failure in the supply chain operation (see Figure 2 on page 19).

Less (Control on) Resources Needed to Handle Risky Situations

The 1990s trends in business, such as outsourcing, just-in-time production, and single sourcing not only put companies in a more risky position, but also limited their ability to manage growing disruptions in their supply chains.

As firms begin to outsource parts of their operation process, they simultaneously experience two other phenomena — loss of control on the resources and loss of visibility across their supply chain.[12] This loss of control and visibility (reflected in the uncertainty about the situation in the supply chain), on one hand, affects the companies' ability to detect disruption and have a full image of the situation. On the other hand, this limits the degrees of freedom they have to cope with abnormality.

Moreover, aiming to identify and eliminate all forms of wastes and buffers in their supply chains, many firms have turned to lean philosophy and reduced the number of suppliers in their supply base. This has resulted in eliminating many, if not all, types of buffers in different forms — finished goods, work-in-process, and raw materials inventory[13] — in the supply chains. However, when the disruptions occur, they have little resources and alternatives to handle shocks and abnormalities.

Higher Impact on Supply Chain Performance

Nowadays, business for supply chains is riskier and the essential resources to handle abnormal events are rare and distributed among different actors. The explicit consequence of this paradoxical situation in managing supply chains is a higher impact on the smooth operation of supply chains. Thus, mangers in the firms must be ready to face different types of disruptions that continuously challenge their constant efforts to improve the performance of their supply chains.

The negative effects of a vulnerable supply chain on the short-term and long-term performance of focal companies are also confirmed by several empirical studies. Based on a large sample —519 glitches announcements made during 1989 to 2000 — Hendricks and Singhal underscore the impact of disruptions in supply chains on the shareholder value. The message is alarming: on average, "supply chain glitch announcements are associated with an abnormal decrease in shareholder value of

(Continued on Page 21)

[11] Charles Perrow, *Normal Accidents: Living with High-Risk Technologies*, Princeton University Press, (1999).
[12] George A. Zsidisin, Gary L. Ragatz, and Steven A. Melnyk, *Effective Practice in Business Continuity Planning for Purchasing and Supply Management*, (2003), http://www.alliedacademies.org/Publications/Papers/JIACS%20Vol%2016%20No%208%202010%20p%201-17.pdf.
[13] Jeffrey K. Liker, *The Toyota Way*, McGraw-Hill, (2004).
[14] Kevin B. Hendricks and Vinod R. Singhal, "The Effect of Supply Chain Glitches on Shareholder Value," *Journal of Operations Management*, 21(2003), 501.

Risk Management *(Cont. from 20)*

10.28%."[14] Another study, based on a sample of 885 supply chain events announced by publicly traded firms, shows how abnormal events have a significant negative impact on the asset utilization, operational performance, and profitability of focal companies.[15]

Higher Customer Expectations

Today, we live in a tough competitive time. Customers constantly demand higher levels of service (higher reliability, near-instantaneous delivery of products, etc.); their expectations are growing every day; and of course, they have more options from global competitors and have more avenues to compare, ascertain opinions, and negotiate pricing than ever before.

For many companies, keeping and losing a customer literary depends on the previous customer's experience with them. Accordingly, customer satisfaction is the essential issue in managing supply chains in many companies willing to compete in the global market.

Nonetheless, modern supply chains seem more vulnerable, complex, and risk-prone; their performance in delivering the customers' expectation is increasingly restrained by many new types of disruptions and uncertainties that must be managed in the daily business. Furthermore, while the customers' expectations alter constantly over time, the change might be easily hindered by lack of visibility in a complex, interconnected supply network.[16]

Final Words: Supply Chain Risk Management

Customer demand for higher levels of service and expectations continue to grow on a daily basis. At the same time, trends in the business world, such as globalization, single sourcing, just-in-time production, and outsourcing, have made business for most international companies extremely risky. How can we handle this paradoxical situation?

For most experts, the answer lays in supply chain risk management: identifying, quantifying, mitigating, and continuously monitoring risk sources across the whole supply chain.

However, for a business culture in which the risk criteria are increasingly traded off against other values such as cost or profitability, it is not easy to accept the concept and implement it in the real-life of their business. Most companies still tend to view risk management and contingency planning as being non-value added. Why? While there are many reasons, two of these reasons standout.

First, linking supply chain risk management efforts to their results is not an easy task. This is mostly because some people may ask themselves: if no accident occurs, is that due to proactive risk management or is it pure luck?

Second, and related to the first point, high-level managers in most companies are not sure that they will receive any bonus for something that might not happen during their management period.

The first point seems a responsibility of scholars; they must present frameworks that support companies to better evaluate the risk management practices. We are also in need of overall-accepted standards as well as detailed best practices for managing risks in supply chains. The second point is more of a practical issue; it calls for a shift in the cultural business and the mindset of companies' board regarding risk management and its contribution to overall strategy of organizations — something that hopefully happens very soon.

At least there is some good news! One of them is presented in a study conducted by IBM. They interviewed 400 senior executives

(Continued on Page 32)

[14] Kevin B. Hendricks and Vinod R. Singhal, "The Effect of Supply Chain Glitches on Shareholder Value," *Journal of Operations Management*, 21(2003), 501.

[15] Kevin B. Hendricks and Vinod R. Singhal, "Association between Supply Chain Glitches and Operating Performances," *Management Science*, 51(2005), 695.

[16] In a report published by Accenture in 2008, 63 percent of those surveyed experienced supply chain disruptions in the past five years and 94 percent said the disruption influenced profitability and affected their company's ability to meet customer expectations ["Keeping Ahead of Supply Chain Risk and Uncertainty," (2008), Accenture and Oracle, http://www.accenture.com/us-en/pages/insight-keeping-ahead-supply-chain-risk-uncertainty-summary.aspx].

Supply Chain Security: With the Requirement for 100% Scanning in Limbo, What are the Implications for the CSI Program?

by Mr. Stephen L. Caldwell, Director of Maritime Security Issues,
U.S. Government Accountability Office (GAO)

Layered Security and 100 Percent Scanning

In the aftermath of the 9/11 attacks, DHS and U.S. Customs and Border Protection (CBP), created a "layered security strategy" to prevent terrorists from smuggling weapons of mass destruction (WMD) in some of the millions of cargo containers shipped into the United States. Among other tasks, these layers included gathering advanced information about shipments, analyzing shipment data to identify high-risk cargo containers, and scanning and physically examining high-risk containers as they arrive in U.S. ports. There are two basic types of equipment to scan containers — that is, to examine the contents without physically opening the container. These include Radiation Portal Monitors (RPMs), which detect the presence of radioactive and nuclear material, and Non-Intrusive Imaging (NII) equipment, which detect density anomalies using X-rays or gamma rays to create an image of the container's contents. Also included in the layered security strategy were new partnerships — working with allied customs officials to identify and scan high-risk containers at overseas ports (known as the Container Security Initiative, or CSI) — in order to expand the U.S. security perimeter beyond our physical borders.

In the early rush to create and expand these programs, planning and internal controls were not well developed and Congress — based in part on a series of GAO and Inspector General reports on the individual programs in the layered security strategy — was concerned about potential security loopholes. In response to these concerns, Congress imposed a statutory requirement that 100 percent of U.S.-bound cargo containers be scanned before being loaded on ships. The containers had to be scanned with both RPM equipment (to detect radiation) and NII equipment (to detect anomalies, including dense materials that could be used to shield radioactive contraband). The scanning requirement was put in place through two pieces of legislation — the SAFE Port Act and the 9/11 Act — which directed CBP to establish selected pilot ports for testing the proposal and to then implement the requirement for all ports by July 2012.

Technology and Pilot Programs Initiated

Even before the statutory requirement was in place, CBP and other components in DHS proceeded to develop technologies and operational pilots to test the feasibility of 100 percent scanning. A variety of new technologies and related improvement programs were initiated, often with very optimistic

(Continued on Page 23)

GAO photos of a foreign container terminal and vessel used to stage and ship some of the millions of cargo containers that CBP screens and scans through its layered security strategy.

Security *(Cont. from 22)*

expectations as to how fast the technologies would be developed, and the level of effectiveness the technologies would achieve. There were several programs.

• **Container Security Devices:** CBP worked with the DHS Science and Technology Directorate to develop four projects to protect the integrity of containers and their contents by detecting intrusions and alarming appropriate officials. Two of these projects were to detect intrusion on all six sides, one of them was to detect intrusion on one side (i.e., the door), and one of them was to communicate the intrusion to appropriate officials. If these projects were successful, they would help prevent terrorists or criminals from accessing containers and introducing WMD or other contraband through either the door or sides.

• **Advanced Spectroscopic Portal (ASP):** CBP worked with the DHS Domestic Nuclear Detection Office to improve RPM scanning through the development of the ASP to replace the hundreds of existing RPM equipment being used by CBP. The ASP would better detect radiation, and then identify the specific isotope in order to determine whether a container was suspicious. Early plans called for using ASP in primary inspection lanes to rapidly scan a large volume of containers.

• **Cargo Advanced Automatic Radiography System (CAARS):** CBP worked again with the DHS Domestic Nuclear Detection Office to improve NII scanning through the CAARS program, which could be used to automatically detect and identify anomalies in cargo density to detect highly shielded nuclear materials in cargo containers. Early plans called on CAARS to be used in primary inspection lanes to rapidly scan a large volume of containers. CAARS would be used in conjunction with ASP to prevent terrorists from smuggling highly-shielded nuclear or radioactive WMD.

• **Importer Security Filing (ISF):** The ISF was not a new technology, but a requirement for additional data from importers and carriers that could be used to better identify high-risk containers. In January 2009, CBP began the program (also known as "10+2" because it required 10 data elements from importers and 2 data elements from carriers). The goal was to better identify those containers that would then receive additional scrutiny through scanning or physical inspection.

In addition, CBP initiated the Secure Freight Initiative (SFI) with operational pilots in several ports: Qasim, Pakistan; Puerto Cortes, Honduras; Southampton, United Kingdom; Hong Kong; Busan, Korea; and Salalah, Oman. These pilot ports included a variety of both smaller ports and larger more complex ports with higher percentages of transshipped containers — containers from one port that are taken off a vessel at another port to be placed on a different vessel bound for the United States. With the passage of the 9/11 Act, the focus of SFI shifted from determining the feasibility of 100 percent scanning to becoming the

GAO photos from 100 percent scanning pilot ports, including mobile RPM equipment in Salalah, Oman (left) and stationary NII equipment in Southampton, UK (right).

(Continued on Page 24)

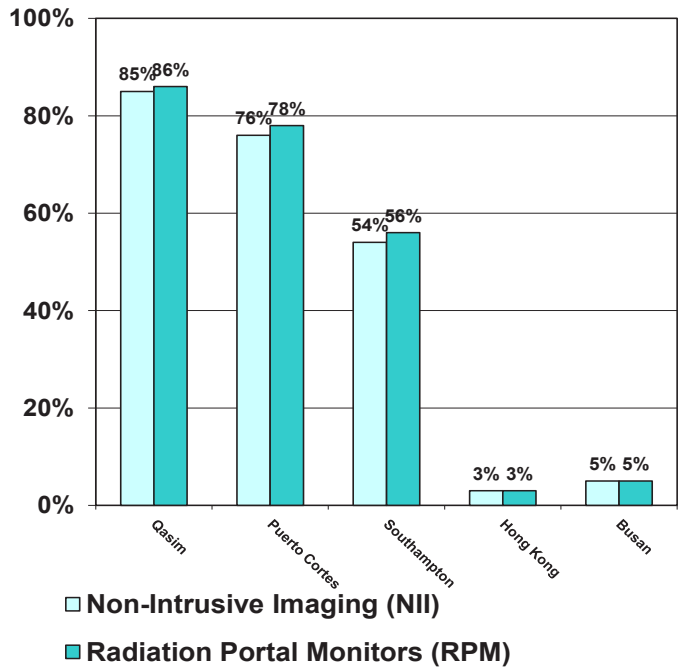
Security *(Cont. from 23)*

first phase in the eventual implementation of the requirement at all ports exporting containers to the United States. CBP was successful in integrating outputs from the various types of scanning equipment with the targeting system used to identify high-risk containers. CBP was also able to use the SFI pilot ports as a testing ground for new inspection technologies, such as mobile RPM scanners and large-scale high-resolution NII scanners.

Technology and Pilots Yield Little Progress

To date, many of the technologies discussed above have not proven to be effective and have generally not been deployed. Of the container security devices, none of the technologies to detect intrusion on all six sides have proven successful. The technology to detect door intrusion, and to communicate the alarm, may have potential and are still undergoing testing. However, CBP would still have to make a variety of difficult decisions on how to deploy these devices, and then get buy-in from other governments and the private sector. The ASP technology did not prove as successful as had been hoped. A series of GAO reports revealed problems in identifying requirements and in conducting operational tests. These reports led to a Congressional requirement that, before DHS fully deploys ASP, the Secretary has to certify that ASPs are significantly more effective than the RPM technology they replace. Testing of ASP continues and DHS has yet to make the certification. Similarly, the CAARS program did not prove successful, in part because the agency pursued the acquisition and deployment of the technology without an appreciation that they would not fit within existing primary inspection lanes at CBP ports of entry. In addition, the CAARS algorithm software did not mature as had been hoped. These factors led to the decision to cancel the acquisition and deployment of CAARS. One exception to the lack of progress was the ISF 10+2 initiative. The program was successful in getting importers and carriers to provide additional data, which CBP has started to use to better assess the risk levels of in-bound containers. In addition, CBP has used one of the newly required data elements (the stow plan) to identify more than 1,000 containers with incorrect manifest data — containers that are inherently high-risk because their contents were not listed accurately on the vessel manifest.

GAO graphic showing the percentage of U.S.-bound containers scanned by NII and RPM equipment at five 100 percent scanning pilot ports.



The SFI pilot ports also produced little progress, and attempts to scan 100 percent of containers have generally been discontinued. Some of the ports that had initially agreed to participate in the SFI program did so for a limited time, or on a limited basis. For example, at the two larger complex ports, Hong Kong and Busan, scanning was done for only about six months at only one of several terminals that ship containers to the United States. Technical and logistical problems at participating ports prevented any of the participating ports from achieving 100 percent scanning, raising doubts about the feasibility and efficacy of the statutory requirement. While CBP was able to scan a majority (from 54 percent to 86 percent) of U.S.-bound cargo containers from the three relatively low-volume ports, it was only able to scan a small amount (from 3 percent to 5 percent) at the two high-volume ports (which together represent about 17percent of all the containers arriving in the United

(Continued on Page 25)

Security*(Cont. from 24)*

States). CBP's most recent budget proposal stated that SFI operations have ended or almost ended in most of the pilot ports and stated that the agency intends to maintain operations in only one SFI port (Qasim).

Costs and Economics Continue As a Barrier

In addition to questions about the technical and logistical feasibility, the current budgetary and economic environment, combined with the potentially high cost of the 100 percent scanning regime, provide additional barriers to implementation. In terms of past spending, CBP and the U.S. Department of Energy identified U.S. costs of $100 million to date for testing 100 percent scanning at the SFI pilot ports. CBP also developed a rough estimate of U.S. costs to fully implement the requirement at $20 billion (based on installing scanners at all ports that export containers to the United States). The $20 billion estimate included initial construction, equipment, and installation costs — not the higher and longer term "life cycle" costs (which would also include operations and maintenance over a period of years). In terms of future spending, CBP's recent budgets reduced funding for SFI from $19.9 million to $3.3 million, as part of a larger reduction in CBP spending on all international cargo scanning programs.

Beyond U.S. costs, governments and terminal operators from Europe, Asia, and the Middle East are generally unwilling to pay for what they see as a U.S.-centric 100 percent scanning regime; however, some of them have borne some of the costs for personnel, infrastructure, and other costs at the initial pilot ports. If 100 percent scanning continues to be implemented, non-U.S. costs could also be substantial. A recent European Commission study estimated European costs at € 430 million (about $617 million) for infrastructure, construction, and equipment costs, and € 200 million (about $287 million) in operations costs per year, including 2,200 additional personnel. In addition to these specific costs, there may be systemic costs through lower terminal efficiency. The European Commission study estimated these annual systematic worldwide economic costs — referred to as welfare loss — at € 150 billion (about $215 billion).

Requirement Remains in Limbo

The demonstrated difficulties and anticipated costs involved in moving forward have put the 100 percent scanning requirement in limbo. DHS and CBP have acknowledged that they will not be able to meet the July 2012 deadline for full scale implementation of 100 percent scanning. They said they will grant extensions to those foreign ports unable to meet the scanning deadline in order to maintain the flow of trade. Under the 9/11 Act, DHS has the authority to grant extensions to any number of foreign ports, which could mean granting a blanket extension to all ports. In addition, senior CBP officials have noted that the 100 percent scanning requirement is not consistent with a risk-based approach. As noted earlier, a further indication that DHS no longer supports 100 percent scanning is that the CBP proposed funding for the SFI pilot ports has dropped significantly and currently supports a single port. Also CPB's budget proposal noted that SFI does not represent a good investment due to its significant costs and many challenges.

Some members of Congress have openly questioned the wisdom of 100 percent scanning at recent hearings. After some such hearings, two bills proposed in the last Congress would revise the 100 percent scanning requirement. For example, last year's Senate bill S.3639 proposed that all U.S.-bound containers be scanned with either RPM or NII, but not both. Similarly, last years Senate bill S.3659 would, upon certification by the DHS Secretary that the current layered security strategy is effective, have waived the 100 percent scanning requirement. More recently, in this Congress, Senate bill S.832 would, again upon certification by the DHS Secretary that the current layered security strategy is effective, only require scanning of containers from "high-risk" ports. These proposed bills show that some legislators are willing to compromise on the original statutory 100 percent scanning requirement.

Hints about the Path Forward

With the 100 percent scanning

(Continued on Page 26)

Security *(Cont. from 25)*

requirement in limbo, where do we go from here? There may be hints in the recent developments, documents, and statements from the White House, DHS, and CBP.

• The White House is developing a new Global Supply Chain Security Strategy, which may provide clear direction on a proposed path forward. The SAFE Port Act required the DHS Secretary to create a comprehensive strategic plan to enhance the security of the international supply chain. In July 2007, DHS published the Strategy to Enhance International Supply Chain Security, which among other items, established a framework for the secure flow of maritime cargo. Now the White House National Security Council is developing a new revised strategy — known as the Global Supply Chain Security Strategy — to replace the 2007 document. The new strategy appears to be an expansion over the original strategy and will include all modes of transportation, all types of cargo, from origin to destination, and both imports and exports.

• DHS Secretary Janet Napolitano spoke earlier this year before the World Customs Organization, emphasizing that DHS wanted to strengthen partnerships with international partners to improve cargo screening and scanning standards and to deploy state-of-the art technologies. The Secretary also called for more coordination of technical assistance to partner nations to ensure they have well-developed, well-equipped customs agencies. She also noted the initiation of project Global Shield, to expand international cooperation to prevent terrorists from using the supply chain to smuggle precursor chemicals for making explosives.

• Customs and Border Protection budget proposals from the last two years indicate changes and reductions. CBP stated that CSI, as currently configured, does not represent a good investment and the agency will reduce operations that do not provide acceptable returns on investment. The most recent budget indicates (without naming specific ports) that CSI will cease operations in several ports while maintaining operations in select ports that prove the most beneficial for scanning high-risk cargo. At the same time, the CBP budget cites a goal to expand operations to new critical international seaports.

Conclusions on Potential Changes to CSI

Overall, these developments and statements provide a couple of themes that hint at the direction the White House, DHS, and CBP may be going with CSI. These themes include (1) the continued expansion of both multilateral and bilateral government partnerships, (2) the shifting of current bilateral partnerships to more strategic high-risk ports, (3) targeting such bilateral partnerships to build capacity and strengthen customs operations, and (4) the leveraging of current technologies and operations to focus on a broader host of contraband. So what specific changes in CSI do these themes indicate with the roll out of the new Global Supply Chain Security Strategy? Here are some potential changes consistent with these general policy pronouncements.

• **Shift CSI Focus to High-Risk Ports:** GAO has recommended that DHS and CBP take a risk management approach in conducting its homeland security missions. Consistent with this, CSI partnerships could be revised to focus on high-risk ports. CSI was originally targeted at ports based on volume of container traffic, not risk. Many of the original 58 ports are in countries that are close allies and have their own robust customs operations. Through CSI, CBP has strengthened relationships and developed trust with these allies. Consistent with recent budget pronouncements, CBP could close operations at some of these ports, and move into new ports considered to have higher risks for terrorists using containers to smuggle contraband. This would also be consistent with the "Strategic Trade Corridor" concept that the DHS Secretary previously approved for the SFI program.

• **Use CSI to Build Capacity:** CSI partnerships could also shift to new ports to build capacity of our less-capable customs partners. CBP could close operations in countries with well-established and robust customs regimes. It could then use these resources to open new CSI operations at ports where the host country customs officials could use help establishing targeting procedures, applying risk management, and using scanning equipment on high-risk

(Continued on Page 32)

Legal Insights

There will be a Tomorrow!

by Steve O'Malley,*
Partner, Analytical Innovative Solutions LLC, and
Coordinator, Ship & Supply Chain Security and Resiliency Standards for International Standardization Organization, TC-8

For the past several years, we have operated in a business climate that has put a premium on cutting all costs, keeping lean inventories, and basically surviving another day. While keeping inventories lean and controlling costs is not about to change, economists are in general agreement that we have hit the bottom and are on the way up in the United States. Also, many countries are much further along into recovery or new growth. Now we need to move from managing merely to survive until tomorrow to managing for long-term prosperity. Chances are that management planning staffs are smaller today than pre-2007 and some subject-matter experts that dealt with specific issues may no longer be employed by organizations. Let us take a look at the multiple threats to supply chains that exist and some of their legal aspects.

When we look at the modern supply chain, we are really looking at production lines. These production lines draw upon numerous material/component, service, utility, and information suppliers and are probably spread across numerous states and countries. Do not think that supply chains simply consist of the trucks that move components to final assembly points. It is important to realize that supply chains are not fixed structures; they are more of a series of short and long-term relationships that come together to meet a business need or opportunity. While organizations may contract with a specific supplier or service provider, the party that actually provides the item or service may be unknown to organizations (subcontractor or slot sharing involvement). Many of these unknown entities will have no impact on operations; however some can affect organizations in a very negative manner.

You Cannot Manage What you Cannot Measure or Do Not Know

The importance of the concept that to manage supply chains, one needs to know their supply chains cannot be stressed enough. Where do they originate, transit through, and end; who is involved; what are the threats to each; and what are the impacts if they are disrupted or corrupted? A positive example of knowing their supply chains was demonstrated by both General Motors and Toyota after the earthquake and tsunami in Japan. Both of these companies were quickly able to identify disruptions to their worldwide operations stemming from damage to the affected region/infrastructure. They were also able to arrange orderly shutdowns or slowdowns of production facilities elsewhere that relied on components from the affected areas until alternative sources of supply could be arranged or the supply chain resumed operation. Unfortunately, the opposite is more common and companies are often surprised by disruptions to their supply chains and are unaware of what can cause the supply chains they depend on to breakdown. A major beverage producer's supply chain chief openly stated that he could not map their supply chains. On a different project, this author, serving as manager, was told that the company shipped product from one port to two ports in the United States and used two ocean carriers. Within hours, it was realized that they were using at least two export ports, a large number of ocean carriers, and up to 14 ports in the United States.

(Continued on Page 28)

Legal Insights *(Cont. from 27)*

If an organization cannot map their supply chains, they will not know what countries are involved, what local issues can disrupt operations, or develop organizational or supply chain resilience.

Let Us Look at Some of the Specific Issues Organizations Should be Worried About

Due Diligence: This is the phrase most hated by project managers (including this author). Organizations ask project managers to deliver something for the lowest possible price, as soon as possible, and to our specifications. When project managers have found the parties that can do just that, the dreaded phrase comes to life. Due diligence needs to assess if there is a reasonable likelihood that the party in question can and will deliver the goods or services needed under the conditions specified while not unexpectedly increasing liability. Just because a supplier or service provider can deliver what is needed does not mean that is what they intend. An aftermarket automotive brake rotor distributor, importing rotors from China, signed an agreement with a production facility that was certified to meet specific quality standards; unfortunately, a company associated with the producer that produced inferior rotors was actually filling the orders until customer complaints led the aftermarket company to investigate.

The past several years have been turbulent to industry. Companies thought to be rock solid have gone under or been merged with others, while some companies have greatly reduced their scope of services or regions served. As a result, due diligence must take a more holistic look: is the company financially sound; do they still have the resources and capabilities to perform what is needed need; are they still delivering the quality needed; are they adequately insured (not just insured to the legal minimum); if they are a transporter, how do they rate in regard to Compliance, Safety, Accountability (CSA) 2010 or port state control scoring; are any involved parties on any of the 90+ Restricted Party Lists that exist globally, and do they have the permits/licenses/authorizations needed?

Failure to conduct proper due diligence increases the likelihood of:

- Goods in transport being held hostage if the transporter/warehouse goes into bankruptcy or creditors seize their assets;
- Goods being seized by the government due to permitting/licensing issues;
- Late or substandard performance by a supplier or service provider;
- Inadvertent use of restricted parties; and
- Companies unknowingly incurring increased liability because their business partner is underinsured (uninsured) or is not considered a safe operator.

Lack of Quality Control: There is a tendency to attempt to assume that business partners are solely responsible for quality within their operation. Unfortunately, the customer or government usually does not see it that way. If the product an organization provided fails to meet expectations, that organization will rightfully be held to blame. If an organization wants to go after someone else, that is their decision. In reality, supply chains are part of organization's production lines, whether they operate them or not. One importer complained to this author about the quality of the products they were having produced oversees. The importer was asked how often their people visited the production facility and he responded "maybe once a year." He was then asked if the production facility was local, how often they would visit it. He replied, "oh probably about every 6-8 weeks." Managing across supply chains is feasible, but requires careful planning and leveraging available tools to control costs. Quality control needs to include a mechanism to quickly identify and isolate defective materials/products/data moving in supply chains to limit damage to overall operations.

Are You Dealing with a Diverter?

A diverter is a party that buys product intended for a market or specific customer and resells it into another market or to another customer. This transaction may be legal or it may be illegal depending on the specifics. Goods produced in the United States for export to foreign markets may be marked or labeled for a foreign market and may not meet U.S. requirements.

(Continued on Page 29)

Legal Insights *(Cont. from 28)*

They may have been produced/ assembled in free trade zones and have not been taxed, and they may have been overseas before being returned to the United States (U.S. Goods Returning). While overseas, these goods may have been stolen, altered, or substituted with counterfeit goods depending on where they were. If a manager is suspicious that they are dealing with a diverter, several questions should asked: are you colluding with one party to defraud another? Are the products acceptable for sale in the U.S. market? Have the goods been tampered with, stolen, or are they out of date? Are the goods subject to unpaid tax liens? Have the goods passed through a restricted party? Are the goods accompanied by the appropriate documents (origin, authorized harvest, etc)?

Are You Managing Customs Compliance? Often, companies will have contracts with customs brokers. They will assume all their customs obligations are being met. However, several issues must be considered. Are corrections to filed entry documents being tracked? Basically, what type of quality management is being applied in regard to customs? If problems occur, this will be a question asked of managers. Foreign customs can present a more interesting challenge. Some customs authorities are corrupt and employed agents moving goods may have adopted practices that would be unacceptable in most countries. Some tell tale signs of this may be that goods are moving over the border and tariffs appear to be paid, yet the customs documents do not indicate who cleared the goods or provide tracking numbers that would indicate the transaction has been entered into the system. Even when the authorities are honest, managers still need to know what assumptions (for example, acceptable variation in volumes) that the broker will be applying to goods and compare them to stated customs policies. When companies wish to audit their shipping practices, the author usually recommends that the project be conducted under an attorney so that attorney work product privileges will apply.

Dangerous Goods/HazMat: For those unfamiliar with the world of dangerous goods, there are two surprises waiting for managers. The first is that most dangerous goods are declared dangerous, classified, and package types selected by the producer of the product (self certification). Self certification is important because a company can slightly alter a non-regulated product resulting in that good now meeting the definition of a dangerous good. If that product is shipped as non-dangerous, the number of violations created can be enormous and pleading ignorance only makes it worse. The other surprise is that the government's definition of the term "shipper" differs greatly from the definition used in industry. This can be very eye-opening. Normally, the party paying the freight is the shipper in industry. The term, when used by the government, is much more inclusive. Each dangerous goods shipment will probably have many "shippers." If dangerous goods that are or will be shipped are touched (figuratively or literally),then the person who touches them is a shipper. Again, pleading ignorance only makes it worse. Basically, the regulation requires companies that produce/ship/handle/package/store dangerous goods to know what dangerous goods are, to be able to classify/package/document them correctly, and to maintain a properly trained work force. In addition, certain safety/security plans may be required.

Supply Chain Resilience: Organizations are served by many supply chains and disruptions to them will cost money. Hardening the chains where feasible and developing strategies to weather a storm and survive are critical to long-term survival. The topic is complex; however, there are tools available that can be leveraged to help manage resilience while keeping costs down.

International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR): Hopefully, a subject-matter expert on these issues has been retained. If not, and a company is involved with engineering, mining, electronics, software, chemicals, military hardware, or hardware used by the military, they need to obtain training on these programs.

If an organization is involved with goods going or moving within the European Union, they need someone with knowledge of their REACH (Regulation for Registration, Evaluation,

(Continued on Page 32)

Resource *(Cont. from 12)*

each scenario is a linear problem, it can be solved by extending Dantzig-Wolfe decomposition (algorithm) of the dual problem and Bender's decomposition of the primal problem to a stochastic programming domain. In other words, the whole stochastic program can be solved by building the combination of outer linearization of the recourse cost function and the master cost function using a cutting plane method. This method is also referred as the L-shaped method.

Managerial Problems and Results

A major challenge that remains is the data acquisition for disaster supply. We received aggregate data from government agencies and more detailed data from private companies comparing ordering and delivery transactions for normal and disaster periods. Further detailed data acquiring is ongoing. FEMA is developing a unified disaster data management system that will include the information needed to build up more realistic scenarios.

The model was solved by considering 30 different scenarios and five key items: water, meal, ice, tarps, and generators. The preliminary results of the "what-if" analysis provided valuable information for three managerial levels. For the strategic level, the cost of the optimal integrated decision was compared with cost of separate decisions. On the tactical level, the preparedness based on expected demand, based on the worst-case scenario, and based on certain reliability level (trade-off between average and worst-case scenario) were considered and compared the cost and service level for the different alternatives. On the operational level, the effect of storage capacity limitations, closed or congested roads leading to modified decisions and cost involved can be studied. ❖

References

Altay, N., and W.G. Green, "OR/MS Research in Disaster Operations Management," *European Journal of Operational Research*, 175 (2006), 475-493.

Bakuli, L.D., and M. Smith, "Resource Allocation in State-Dependent Emergency Evacuation Networks," *European Journal of Operational Research*, 89 (1996), 543-555.

Barbarosogcaronlu, G., and Y. Arda, "A Two-Stage Stochastic Programming Framework for Transportation Planning in Disaster Response," *Journal of Operations Research Society*, 55 (2004), 43-53(11).

Drager, K.H., G.G. Lovas, and J. Wiklund, "Evacsim: A Comprehensive Evacuation Simulation Tool," Emergency Management and Engineering Conference 101-108, (1992).

Kongsomsaksakul, S., A. Chen, and C. Yang, "Shelter Location-Allocation Model for Flood Evacuation Planning," *Journal of Eastern Asian Society for Transportation Studies,* 6: (2005), 4237-4252.

Liu, Y., X. Lai, and G. Chang, "Two-Level Integrated Optimization System for Planning of Emergency Evacuation," *Journal of Transportation Engineering*, 132(10), (2006), 800-807.

Liu, C., Y. Fan, and F. Ordonez, "A Two-Stage Stochastic Programming Model for Transportation Network Protection," *Computers and Operations Research*, 36, (2009), 1582-1590.

Saadatseresht, M., A. Mansourian, and M. Taleai, "Evacuation Planning Using Multi-Objective Evolutionary Optimization Approach," *European Journal of Operational Research*, 198(1), (2009) 305-31.

Sherali, H.D., T.B. Carter, and A.G. Hobeika, "A Location-Allocation Model and Algorithm for Evacuation Planning Ender Hurricane/Flood Conditions," *Transportation Research Part B: Methodological*, 25(6), (1991), 439-452.

Stepanov, A., and J.M. Smith, "Multi-Objective Evacuation Routing in Transportation Networks," *European Journal of Operational Research*, 198(2), (2009), 435-446.

Tufekci, S., "An Integrated Emergency Management Decision Support System for Hurricane Emergencies," *Safety Science*, 20(1), (1995), 39-48.

Yi, W., and L. Ozdamar, "A Dynamic Logistics Coordination Model for Evacuation and Support in Disaster Response Activities," *European Journal of Operational Research*, 179, (2007), 1177-1193.

Critical Infrastructure *(Cont. from 8)*

can claim the right to modify the infrastructure to their needs. In general, we can reduce the risk of critical infrastructure failure through the following:

- **Protection and Hardening against Hazards:** Increase redundancy, build in backup or alternate systems or processes.

- **Reduction of Vulnerability:** Eliminate single points of failure, use best-in-class providers to eliminate weak areas, and mitigate the most likely hazards.

There will be times, however, when the critical infrastructure will fail regardless of what preventive measures are in place. In those cases, we can minimize the impact of that failure by having a robust incident management and continuity of operations plan (COOP).

With a risk model in place, management can make decisions on the tradeoffs between improving the reliability of critical infrastructure against the related costs. In other words, identifying and managing toward an acceptable level of risk. In some cases, the risk to a supply chain due to infrastructure can be significant enough to warrant actions from the commercial sector, such as influencing industry regulations or government industrial policy. These treatments require more effort to realize and typically require a broad collaboration among infrastructure managers and potentially other industry associations. Through these mechanisms, commercial infrastructure users can advocate for investment in infrastructure maintenance or upgrades to the infrastructure using new designs or new technologies.

Critical infrastructure is a supply chain enabler and its reliability is increasingly important in the effective and efficient functioning of the supply chain. With improvements in technology come increasing demands for speed, customization, and lower costs. Subsequently, the further organizations stretch to meet demand, the greater the potential impact of disruptions due to critical infrastructure failure. Minimizing critical infrastructure risk can ensure supply chain costs remain predictable and as low as possible while maintaining reliable performance. The greater the critical infrastructure reliability, the lower the level of contingency is required, and the leaner the entire operation.

Using a SCRM approach to understanding how critical infrastructure interacts with the supply chain provides an understanding of the interrelationships between critical infrastructure management and supply chain resilience. Supply chain and infrastructure managers share a common interest in maintaining a reliable and effective infrastructure. When the commercial and public sectors work together to prevent the failure of critical infrastructure, the entire economy benefits. ❖

Rich Skulte is a Program Manager in LMI's Infrastructure and Engineering Management group. He has more than 20 years of experience in program and project management, infrastructure engineering, facilities and asset management, and business process improvement. Mr. Skulte oversees multiple asset management projects for federal clients including infrastructure condition assessments, real property master planning, business transformation, and recapitalization program support. Mr. Skulte is a Project Management Professional (PMP), has a BS in Electrical Engineering from The New Jersey Institute of Technology and an MBA from the McDonough School of Business at Georgetown University.

Taylor Wilkerson is a Senior Consultant in LMI's Supply Chain Management program where he supports clients in supply chain optimization, risk management, information management, and sustainability. Mr. Wilkerson works with Federal clients, the Supply Chain Council, the Council for Supply Chain Management Professionals, and the Supply Chain Risk Leadership Council to identify and implement best practices in supply chain risk management. Mr. Wilkerson has a BE in Mechanical Engineering from Vanderbilt University and an MBA from the Robert H. Smith School of Business at the University of Maryland, where he is currently a Senior Fellow.

Security *(Cont. from 26)*

containers. Some of these ports may also be high-risk ports, as discussed above. In addition to strengthening local customs operations, such new CSI operations could help to expand and strengthen CBP's overall relationship and trust with these foreign customs agencies.

• **Leverage CSI Beyond WMD**: While CSI has always had a focus on detecting WMD, GAO has recommended that DHS determine the feasibility of expanding CSI to target and scan containers for illicit drugs in major drug transit zones. Expanding CSI in this way would help maximize cargo container assistance to other countries, and potentially yield benefits to international counternarcotics efforts. In addition, the DHS Secretary announced the Global Shield initiative to expand supply chain security programs to interdict precursor chemicals used in the manufacture of improvised explosives devices — one of the most common devices used by terrorists in attacks. While CSI was originally developed and proposed to our allies as exclusively focused on WMD, many of our CSI partners have recognized the benefits of CSI targeting and scanning across a variety of law enforcement activities. In these times of budget austerity, CSI resources could be leveraged by expanding beyond WMD to interdict counternarcotics, explosive precursors, and other contraband. ❖

NOTE: The author based this article on a series of GAO reports, including "Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers" (GAO-10-12). See www.gao.gov/cgi-bin/getrpt?GAO-10-12.

Legal Insight *(Cont. from 29)*

Authorization and Restriction of Chemicals) program.

Today, the world is more integrated than ever before. This has produced great efficiencies for all people. However, it also means that threats, natural or manmade, previously assumed to be far away, must now be considered. Our industry is challenging. Unless we keep up with those challenges, we will likely suffer costly consequences. ❖

*Steve O'Malley is a partner in Analytical Innovative Solutions LLC and is also the Coordinator for Ship & Supply Chain Security and Resiliency standards for International Standardization Organization, TC-8. Previously he was the Director, Maritime & Supply Chain Security with Science Applications International Corp*oration *and is a retired US Coast Guard officer. He has a Master Degree in Transportation Management from Florida Institute of Technology and an undergraduate degree from Central Connecticut State University. He can be contacted at aninso.llc@gmail.com.*

Risk Management *(Cont. from 21)*

from different parts of the globe, from North America to Asia Pacific region, who are responsible for their organizations' supply-chain strategies and operations.[17] One of the key findings of this study is extremely fascinating and inspirational: "[r]isk management emerged as supply chain executives' second most common concern." ❖

[17] Karen Butner, "The Smarter Supply Chain of the Future," *Strategy and Leadership*, 38 (2010), 22.

Operational *(Cont. from 16)*

the generation of supply chain tracking information, using a Hidden Markov Model, and the decision-making process based on said model
b. Quantification of the value of tracking information in monetary terms.
c. Analysis of the impact of information accuracy and information granularity on the value of information, together with the implications that these have on the selection of the appropriate technologies in tracking systems.
d. A step-by-step method for evaluating tracking systems in industrial cases.
e. Three case studies that demonstrate how the proposed model and methods can be used to evaluate and compare tracking systems in a real industrial setting, demonstrating the shortcomings of existing systems and suggesting key improvements methods can be used to evaluate and compare tracking systems in a real industrial setting, demonstrating the shortcomings of existing systems and suggesting key improvements.

Food Safety *(Cont. from 10)*

prepared foods.[6] While these statistics are negligible for the greater U.S. food supply, this case underscores the continued need to do more to protect American consumers from the global food supply chain risks. In particular, the FDA must step up its regulatory and surveillance of food imports into the United States. Our food supply is perhaps among the most critical of our infrastructures. Albert Einstein once posited, "[w]hat must a fish know about the water in which it swims?" The answer is that the fish needs to know nothing, but those responsible for its safety and security [of the fish] with regard to global food supply chain management had better know everything.

Recalling the four critical elements of a global supply chain, we need to know if the fish itself is safe, who is moving the fish through the supply chain, how the supply chain is financed, and how it is being delivered from point to point. Stakeholders in global supply chain management across all industries, not just food, must continue to set and improve international standards and strive towards instilling public trust in the government or private agencies charged with safeguarding these supply chains. ❖

Celina Realuyo has dedicated her career to the practice and promotion of international relations, as a U.S. diplomat, international banker with Goldman Sachs, senior U.S. foreign policy maker, and professor of international affairs at Georgetown, George Washington, and the National Defense University. She has extensive expertise in the international security, geopolitical risks, globalization, illicit economies, international banking, economic competitiveness, business development, and government relations arenas. Celina hold an M.B.A. from Harvard Business School, M.A. from Johns Hopkins University School of Advanced International Studies (SAIS), and B.S. from Georgetown University School of Foreign Service. She has visited over 50 countries, speaks French and Spanish fluently, and is conversant in Italian, German, Filipino, and Arabic.

---

[6] Renee Johnson, "Japan's 2011 Earthquake and Tsunami: Food and Agriculture Implications," *Congressional Research Service*, (April 13, 2011), 2 and 7.

Management *(Cont. from 3)*

opportunities in Philadelphia, Pennsylvania. It is the largest supply chain management event in the world. Do not miss this year's keynote speaker, FOX Business Network Anchor, Stuart Varney, who will present *Plain Talk on the Global Economy*. Registration for the conference is available at cscmpconference.org. ❖

For more information, contact CSCMP at 333 East Butterfield Road, Suite 140 Lombard, Illinois 60148-5617. CSCMP can also be contacted by telephone at (630) 574-0985 and email at membership@cscmp.org.

Rick D. Blasgen currently serves as the president and chief executive officer of the Council of Supply Chain Management Professionals (CSCMP) in Lombard, Illinois.

He began his career with Nabisco, where he held various logistics positions of increasing responsibility in inventory management, order processing, and transportation and distribution center operations management. He became vice president, supply chain, at Nabisco in 1998, then vice president supply chain for Kraft in 2002. From 2003 until 2005, he served as senior vice president integrated logistics at ConAgra Foods.

He earned his degree in business administration from Governors State University.

Volatility and Risks *(Cont. from 5)*

Conclusion

We enjoy the benefits of the global supply chain through the goods we purchase as consumers, and through the parts and equipment our businesses needs to grow. The benefits may be outweighed by the risks inherent in the global supply chain. We can become over reliant but not be aware that we are until after a disaster occurs. How we develop and implement tools to guide global supply chains will impact our personal and national economic lives. ❖

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1