Supply Chain Management

Viewpoint

High performance: Ensuring global freight security

New strategies for safe and innovative supply chain management

accenture

High performance. Delivered.

By Jade Rodysill

Despite their potential effectiveness, emerging global security policies have real potential to further constrain the operations and resulting profitability of many organizations. To prevent this from happening and ensure their competitive positioning on the path to high performance, organizations need new supply chain management approaches to global freight security. This point of view identifies three innovative strategies to help global entities mitigate and even exploit new freight-movement guidelines.

• Consulting • Technology • Outsourcing

Commercial enterprises have grown accustomed to complying with regulatory efforts—particularly those focused on the security of personnel. However, increased attention is also now placed on the global movement of freight and its associated informational and financial flows. Recent examples include the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Hazardous Materials Vulnerability Reduction Act of 2005, which seek stiffer penalties for noncompliance.

Around the world, regulators and legislators are paying more attention than ever to individual shipments, thus adding more complexity to an already dizzying activity. Even before new regulations, a typical cross-border shipping process involved 35 documents and 25 parties—all of which were subject to more than 600 laws and 500 regulations.[1]

Despite their potential effectiveness, emerging global security policies have real potential to further constrain the operations and resulting profitability of many organizations. To prevent this from happening and ensure their competitive positioning on the path to high performance, organizations need new supply chain management approaches to global freight security.

This point of view identifies three innovative strategies to help global entities mitigate and even exploit new freight-movement guidelines:

1. Design a layered, open, flexible and tightly coupled security model

2. Implement a continuous "sense and respond" capability

3. Conduct closed-loop planning and advocacy

As the number and complexity of regulations continue to rise, organizations cannot afford to overlook the value in realizing effective freight security operations and incorporating this critical element into their supply chains. For most organizations, security has yet to arise to the forefront of supply chain management. However, leading companies are getting ahead of the curve by first and foremost obtaining a comprehensive understanding of the current dynamics in the regulatory environment. They think strategically about how freight. security can impact their enterprise, and then identify and capture opportunities to ensure security and profitable growth. In this way, they exhibit one of the key characteristics of high-performance businesses.

According to Accenture's ongoing research into the supply chain mastery behaviors of high-performance businesses, high performers rigorously execute against their strategies and capabilities, and constantly adapt them to changing market needs, such as those associated with freight

[1] World Trade Organization (WTO), July 2005

Emerging global security policies have real potential to further constrain the operations and resulting profitability of many organizations.

security. High-performance businesses consistently outperform their peers in revenue, profit growth and total return to shareholders despite industry disruptions, business cycles and new leadership. In a market riddled with constant change, particularly with regards to the freight security regulatory environment, a company's supply chain can spell the difference between success or failure.

Adopting the three anchor strategies detailed in this point of view can help organizations build supply chains that are information-rich, technologically robust, tightly integrated and highly flexible. In this way, they can master the type of distinctive capabilities that are critical to achieving high performance in today's dynamic and expanding economy.

Changing dynamics

For the United States, September 11 was a tipping point in the management of security for personnel and inbound product. Heading the list, the U.S. Department of Homeland Security (DHS) was created, and its sphere of influence steadily expanded through a patchwork of agencies. Since 2001, the Transportation Security Administration (TSA)—which was originally in the Department of Transportation but moved to DHS in March 2003—has spent more than $11 billion on airline passenger security.[2] However, its commitment to freight security has been far smaller. Less than 10 percent of the estimated $7.3 billion needed to meet United States port-security requirements has been secured.[3] Principal reasons include:

- Human value: The foremost need clearly—and correctly—has been to provide increased security to people traveling or gathering in public forums.
- A reactionary strategy: The federal government's primary approach has been to respond to threats, not to proactively position itself against them.
- Commendable performance: Although the United States' commercial transportation network is large and complex, more than 99.5 percent of HAZMAT shipments via rail are delivered without incident.[4]

This is not to say that freight security buy-in has been wholly lacking: DHS-sponsored programs such as C-TPAT currently have nearly 6,000 members. The Container Security Initiative (CSI) comprises more than 40 member ports. And the Free and Secure Trade (FAST) Program includes more than 15 border crossings.[5] Moreover, some benefits have accrued through programs like FAST, which can save motor carriers between 40 and 90 minutes per border crossing if physical capacity is sufficient.[6] Collateral benefits also have been realized in the form of reductions to the $30 billion in annual United States cargo theft

[2] The White House, October 2004
[3] U.S. Coast Guard, October 2004
[4] American Association of Railroads and Pipeline and Hazardous Materials Safety Administration (PHMSA), 2004
[5] The Free and Secure Trade (FAST) Program is a joint Canada-United States initiative involving the Canada Border Services Agency and the United States Customs and Border Protection (CBP). FAST supports moving preapproved eligible goods across the border quickly and verifying trade compliance away from the border. It is a commercial process offered to preapproved importers, carriers and registered drivers. Shipments for approved companies, transported by approved carriers using registered drivers, will be cleared into either country with greater speed and certainty, and at a reduced cost of compliance. Source: The Free and Secure Trade (FAST) Program, www.cbsa-asfc.gc.ca/import/fast
[6] CBP and *Logistics Management*, 2004

(the result of tightened security and the improved asset utilization enabled by mobile resource management technologies), as well as reduced insurance premiums due to lowered risk exposure and increased asset utilization through improved visibility.[7] However, two issues remain prominent: 1) enforcement is lacking, and 2) freight security is increasingly costly and delay-prone.

Lack of enforcement

Thus far, only 11 percent of C-TPAT members (the premier DHS program) have been validated, despite the agency's three-year goal to validate all members, as established by the U.S. Customs and Border Protection (CBP) agency.[8] Compared to non-members, C-TPAT members are one-sixth as likely to have their imports inspected and one-fourth as likely to be chosen for customs compliance exams.[9] However, the increased number of inspections post-9/11 has diluted much of the anticipated benefit.

Rising costs and greater delays

Inbound container-inspection rates have increased from 2 percent pre-9/11 to greater than 7 percent in some major ports, with delays of up to 21 days incurred for containers that fail to pass pilot programs, such as the Vehicle and Cargo Inspection System (VACIS).[10] It is calculated that the annual cost of slowing the delivery of imported goods by just one day could reach $7 billion[11], while delays already anticipated are expected to require upwards of an additional 5 percent—$75 billion—in buffer stock.[12]

[7] Pinkerton Consulting & Investigations, July 2004
[8] CBP, 2004
[9] CBP, 2004
[10] CBP New York Office, February 2005
[11] The Brookings Institution, May 2005
[12] State of Logistics Report, 2003

Despite the security benefits of new legislative efforts, many shippers will likely be saddled with increases in delays, direct investment, administrative costs, opportunity costs and risk management.

In addition, C-TPAT enrollment requires an average start-up investment of $200,000 and two-thirds of that amount to maintain annual compliance.[13]

Regulatory and legislative efforts and impacts

Numerous efforts are being made to surmount the above problems. For example, new, increasingly aggressive administrations at DHS, CBP and TSA are focusing more tightly on freight security and working to eliminate security breaches. Lawmakers have been introducing legislation to increase the transparency and accuracy of informational and financial flows, and to harden physical security in response to public sentiment. Despite the security benefits, many shippers will likely be saddled with additional costs and other inconveniences. These include increases in:

Delays

Motor carriers entering the United States from Mexico now have to electronically transmit more-detailed shipment information to the CBP. The resultant burdens on data processing (~126 data elements versus the former 12) have increased delays, particularly since fewer Mexican draymen are available to haul loads. Most draymen are owner-operators who will not have the financial resources to make the required technology investments.[14]

Direct investment

Phase 1 of the revised C-TPAT requirements called for a high-security seal (certifying compliance to current PAS ISO 17712 standards) to be affixed to all loaded containers bound for the United States. Legislation also has been introduced that would require 50 percent of containers entering the United States to meet a "smart box" standard by 2007.[15] (See the accompanying sidebar to learn more about "smart" containers and cargo monitoring technology.)

Administrative costs

Phase 3 of the revised C-TPAT requirements demands members develop written and verifiable security processes, as well as documentation certifying that their business partners are meeting C-TPAT security criteria.[16]

Opportunity costs

Several municipalities are introducing laws to limit the routing of some hazardous materials. In response to concerns about limiting interstate commerce, the United States Senate introduced the Hazardous Materials Vulnerability Reduction Act of 2005 to provide coordination of HAZMAT rerouting at a national level.

Risk management

A constantly changing list of more than 50 "denied parties" must be referenced for each shipment. Moreover, legislation seeking to curtail global money laundering and terrorist financing (for example, Section 326 of the Patriot Act) requires businesses to verify customer identities.

[13] *Logistics Management*, 2004
[14] *Logisitics Management*, June 2005
[15] CBP and the Intermodal Shipping Container Security Act, 2005
[16] CBP, 2005

"Cargo monitoring" technology can detect security threats

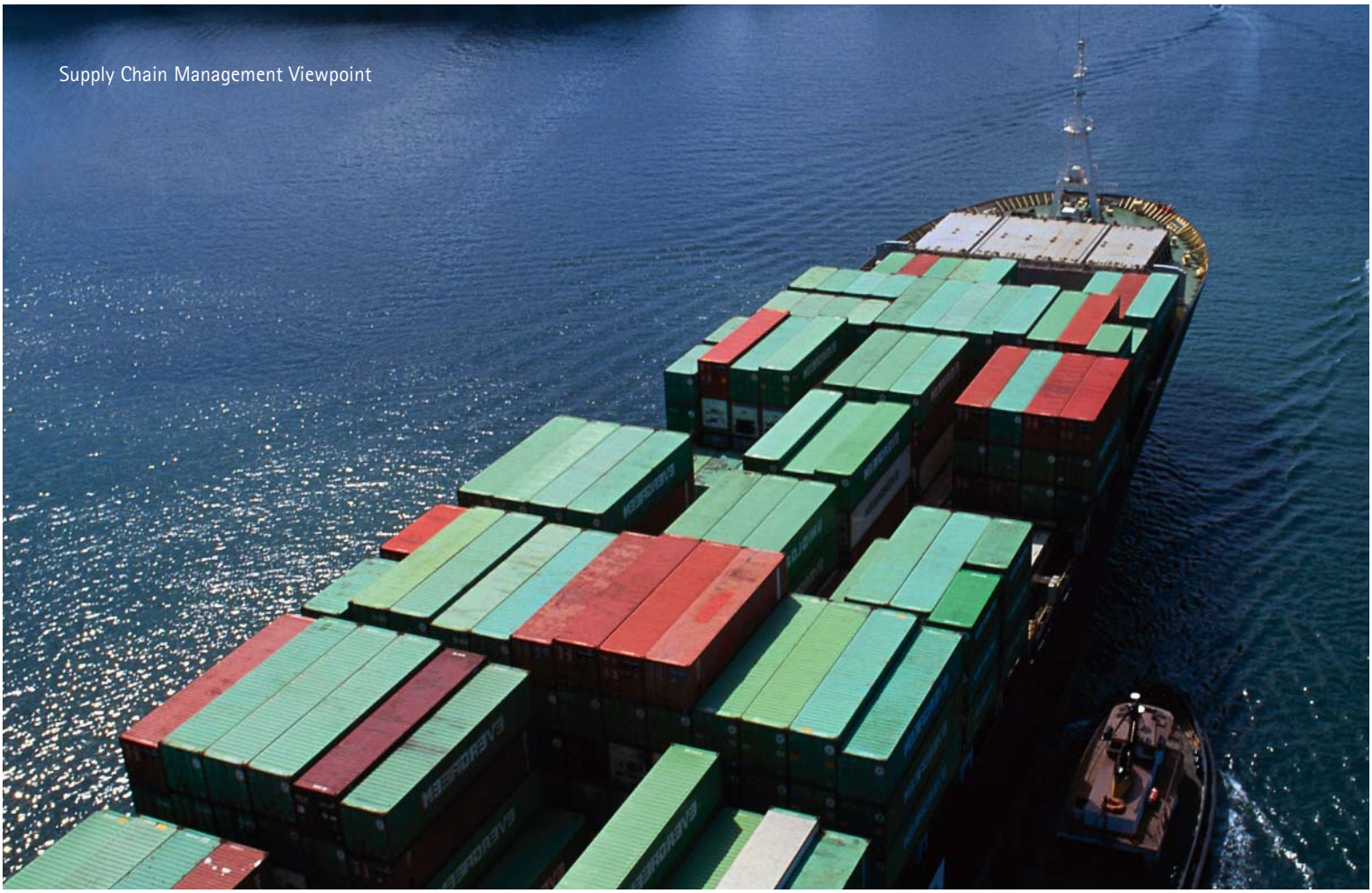
Ninety percent of the world's cargo moves by shipping container. If a security breach involving containerized cargo caused ports to be closed, it could have devastating economic consequences worldwide. With its cargo monitoring prototype, Accenture Technology Labs is investigating how a limited number of sensors could be used to shore up vulnerabilities that exist in shipping networks without requiring extensive infrastructure investments.

The prototype can detect potential threats using radiation sensors mounted on containers. When a threat presents itself, the prototype uses a mesh network (a flexible architecture for moving data efficiently between devices) to communicate sensor data to a security application. In practice, a subset of these "smart" containers would also be satellite-enabled, allowing them to communicate even when local ports are not equipped with mesh networking infrastructure. Suspect containers would then be "marked" as having a high threat level. As the suspect container makes its way to its destination it would be stopped for inspection.

What makes the approach pioneered by the cargo monitoring prototype unique is that one container can monitor the neighborhood of containers around it. As a container with a potential threat moves through the system and is observed by multiple equipped containers, it can effectively narrow down which containers may contain likely hazards and effectively focus limited inspection resources.

In addition to a physical proof of concept, the Labs has conducted simulations to gauge the effectiveness of this approach. The simulations considered several scenarios with varied rates of instrumented containers and a varying rate of inspections at the ports. So far the results have been positive. In preliminary simulations using a 10-foot sensing range with a penetration rate of 5 percent and a 3 percent port inspection rate, the technology had an 80 percent chance of detecting a container threat. Increasing penetration to 10 percent improves the chances of detecting a container threat to more than 90 percent.

As organizations consider cargo monitoring systems that involve instrumenting containers, this approach may offer a way to improve security while coping with the economic reality that instrumenting every container is simply unattainable in the near term future—and perhaps even unnecessary.



The most successful security models are those that are layered, open, flexible and tightly coupled.

Recommended strategies

It is easy to see that freight security will be more complex than ever in the coming years. This outlook is clearly apparent when combining the aforementioned regulatory and legislative efforts with such external forces as constrained refining capacity; shifting centers of sourcing, production, and consumption; and stronger regional trading blocs. In response, organizations engaged in global trade must develop supply chain models that simultaneously minimize risk exposure and maximize speed to value. These actions also should be supported by enhanced visibility into security and into the consequences of actions taken.

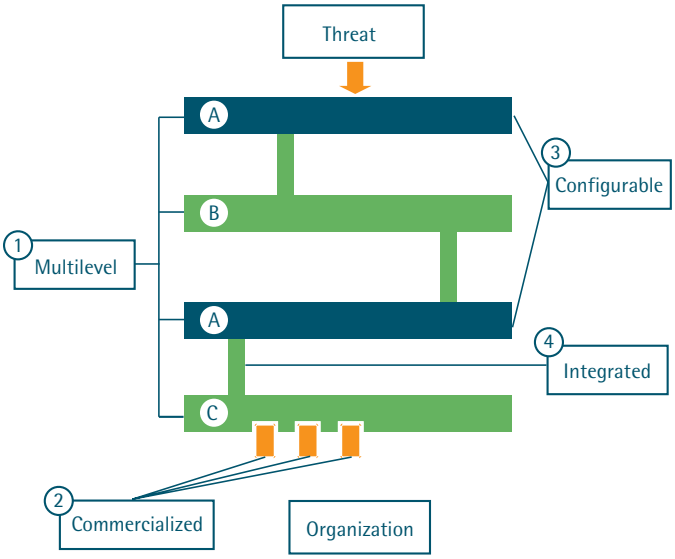
The following three strategies are particularly useful in helping organizations navigate through a murky and complicated future.

Design an optimal security model

The most successful security models are those that are layered, open, flexible and tightly coupled. Layering, or implementing multiple security solutions, is particularly important since no one layer or solution can be expected to fend off all threats. Five layers that each are 60 percent effective represent 99 percent effectiveness in the aggregate [(1-(1-.6)^5)]. However, two layers that are individually 80 percent effective are only 96 percent effective in the aggregate. A good way for C-TPAT members to operationalize this concept is to make compliance with CBP requirements (for example, written and verifiable processes) a contractual obligation for their importers. By holding partners to tightly defined security procedures, entities are creating a layered model with more predictable efficacy.

Figure 1

Key characteristics of an optimal security model



1. Multilevel: A reliable security solution must comprise multiple levels of individual security components. A single layer, no matter how well engineered or perceptibly holistic, cannot match the redundancy provided by multiple solutions and avoids the catastrophic single point-of-failure scenario.

Layered

2. Commercialized: Beyond simply offering a more proven and more readily integrated solution, commercialized (open) security components present organizations with real options. Security regulations are highly dynamic and expected to remain so for the indefinite future. By employing only commercialized components, compliance risk is shifted to the vendor.

Open

3. Configurable: In addition to being commercialized, the individual security components should be highly and easily configurable. Needs change over time, and sometimes rapidly in response to world events/shocks, thus necessitating configurability.

Flexible

4. Integrated: To maximize value, the individual components layered into the security model must be tightly integrated. Such integration enables the creation of a "sense and respond" capability, increasing response velocity (speed + trajectory). The use of commercialized components assists integration efforts.

Tightly coupled

An optimal security model is based on an open architecture that leverages innovative yet commercially viable technologies. Vendors are regularly introducing novel applications, such as smart containers, seals and VACIS standards. By using these commercialized components, organizations can create a solid foundation for integration. This also means the risk of ensuring compliance remains with the supplier, thus creating real options for organizations to enter, expand, contract and exit positions with acceptable risk exposure and tolerable amounts of investment dollars.

For several reasons—but particularly to ensure an organization can accommodate changes over time—flexibility is a core feature of the model. On the one hand, entities such as the World Customs Organization (WCO) demand flexibility in process enablement and parameter setting. However, tailored responses also are needed to comply with, say, the European Union's Waste Electrical and Electronic Equipment (WEEE) Directive, or mandates from the Agricultural Department's Animal and Plant Health Inspection Service, as well as the International Plant Protection Convention to appropriately treat wood packaging for pests and mark materials accordingly. A security model's flexibility is what enables organizations to respond quickly and effectively to cataclysms or unexpected rulings from various governing bodies. After all, high-performance businesses create and nurture a supply chain organization that anticipates and drives change, rather than reacts to it.

The final characteristic of an optimal security model is tight integration, which ensures benefits are realized by employing multiple layers, commercialized components, and built-in flexibility and configurability. Tight integration also improves visibility and reduces data variability, thereby improving asset utilization and reducing inventory.

The key is adopting a comprehensive approach to freight security from "sense" through "respond."

Conversely, failure to create interfaces among key solution components is certain to extend delays. A good example is the Automated Commercial Environment (ACE) system for prearrival notification, which is required to maintain FAST Green Lane status.[17]

Addressing the above criteria when designing a security model can help organizations operate securely and cost-effectively, respond quickly and appropriately to threats, and achieve higher levels of performance. Multiple solution layers increase the probability of being protected, while integration accelerates organizational responses. Furthermore, configuration and commercialization help ensure cost-effective, flexible responses as environments change. High-performance businesses realize failing to incorporate these criteria could result in higher insurance premiums, increased risk of cargo theft and the loss of C-TPAT's preferred processing benefits during elevated threat periods.

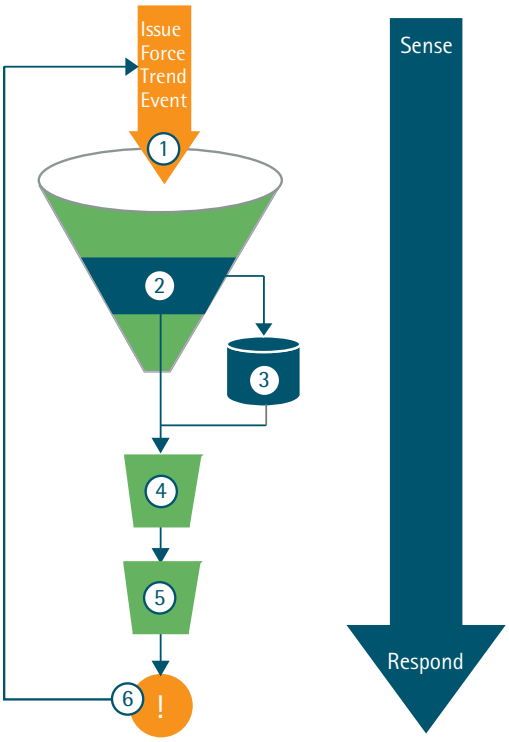
Implement a continuous "sense and respond" capability

A primary security tenet is the ability to pick up and interpret signals, and then to respond quickly and appropriately based on rapid operational and financial-impact analyses. This "sense and respond" capability will become even more vital as the frequency of regulatory events increases geometrically, the required time-to-action gets shorter and signal-to-noise ratios decrease (the difficulty of distinguishing valuable information from increasing amounts of post-9/11 clutter and hyperbole). Process templates and technologies already exist to make this happen. The key is adopting a comprehensive approach from "sense" through "respond."

With a typical cross-border shipment already subject to compliance with some 500 trade agreements and 600 laws, it clearly is necessary to identify, capture and filter information in advance of physical and financial flows. This "sensing" capability means recognizing the conditions under which influential events might occur. It also implies the capacity to interpret information, not just capture it. For example, London authorities benefited from the visibility provided by numerous video cameras and the awareness that a tragedy similar to the London subway attacks occurred the previous year in Madrid. Yet a lack of rapid, insightful interpretation prevented meaningful action.

[17]ACE is the next generation of technology designed to enhance national border security and expedite lawful trade. It automates and consolidates border processing. Through tools like the ACE Secure Data Portal, unprecedented integration of information and communication between CBP, the trade community and other participating government agencies is provided through a single, integrated, online access point. Source: U.S. Customs and Border Protection, http://www.cbp.gov/xp/cgov/toolbox/about/modernization

Figure 2
Continuous sense and respond capability



1. Collect and monitor: The convergence of the Internet with emerging technologies like agents, spiders and crawlers enable organizations to more proactively monitor a broad array of issues, forces, events and trends of a potentially significant impact.

2. Interpret: High-performance organizations employ pattern-recognition techniques like fuzzy logic and other artificial intelligence techniques like neural networks, not to mention standard data mining, to provide rich, rapid interpretation of inbound signals and a thorough threat assessment.

3. Alternative response generation: Based on the threat assessment, alternative responses—predefined or ad hoc—are automatically assessed for feasibility. A small number of "top" responses are selected.

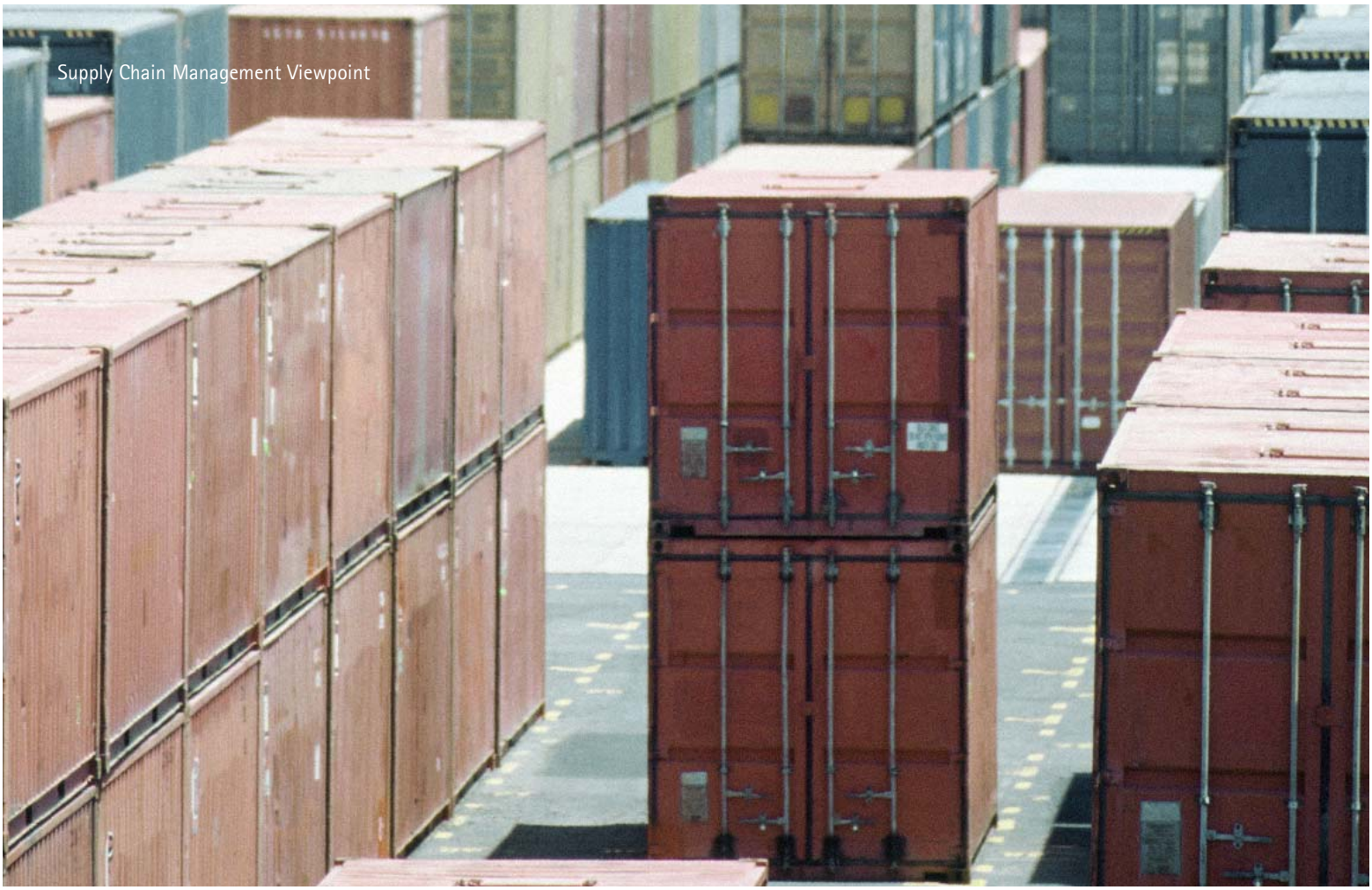
4. Simulate operating impact: For each of the "top" responses, the associated operating impact is estimated by simulating changes to key financial metrics and then mapping aggregate impacts to pro-forma financial statements.

5. Simulate financial impact: For each of the "top" responses, the associated operating impact is estimated by simulating changes to key operating metrics.

6. Decide and act: Based on both the expected operational and final impacts, organizations select and act upon the "best" response.

All in all, greater interpretative capabilities will require new techniques and technologies for viewing changes in data over time (trends, inflections) and in comparison with other data (correlations, fuzzy logic). Quickly, yet comprehensively, organizations will then be able to: 1) formulate potential responses; 2) evaluate the relative impact of those options; and 3) take appropriate action.

Together, the above three "respond" capabilities imply a fundamental realization: Alternate responses can be preconfigured and refined over time. (Consider that a lack of "preformulated" responses lessened the utility industry's ability to prevent and then restore power following the Northeast's dramatic outage in 2003.) Such responses first require an operational perspective: determining if there will be any delayed or tertiary impacts across an organization's network and those of its partners. Tackled next from a financial perspective, response formulation could include large-scale modeling of cost-to-serve impacts, lost-opportunity costs and/or the effect on warranty costs if order covenants are broken. Such simulations give management an explicit, critical understanding of both the probable range of outcomes and the potential tradeoffs between cost and service.



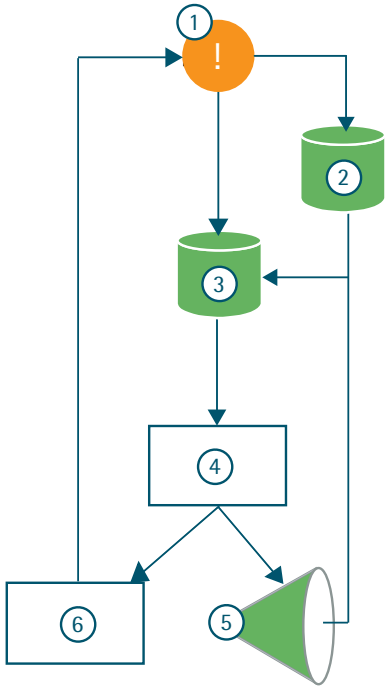
Closed-loop planning helps ensure feedback that is immediate, insightful, actionable and meaningful.

Conduct closed-loop planning and advocacy

This security strategy is geared to helping organizations learn from experience by doing a better job of monitoring decisions and then evaluating associated impacts and reactions. It also means scrutinizing environmental conditions, recording those observations and using them to build dynamic models that improve the future effectiveness of security plans. Savvy executives know the key to continuously selecting and enacting the right responses lies in understanding the outcomes of their own organization's actions, along with the counteractions of other organizations and regulating entities. This insight demonstrates one of the characteristics of high-performance businesses: High performers excel at consistently making the critical decisions that give them the right strategic direction and a winning market focus and position.

The first step of this strategy is simply to capture—or diligently record—the decision, relevant inputs and outputs, the outcome, and key environmental variables present at the time of the decision. Once such a foundation is established, an organization can develop models that help it understand the impact of refinements to past and proposed actions. Oil increases of 50 percent seemed unfathomable a year ago, so very few companies were prepared. Nor were many organizations ready for China's rapid emergence as a consumer of almost a third of the world's steel and coal. Models for assessing the impact of supply shocks and seismic commercial shifts point the way to new and better courses of action. They also help organizations ensure consistency, quality and repeatability. Leaders understand this closed-loop process of "act, document, model,

Figure 3
Closed loop planning and advocacy



1. Decide and act: The "best" decision, as executed by the continuous sense and respond capability, initiates the strategy behind closed loop planning and advocacy.

2. Record decisions, outcomes and environmental variables: High-performance businesses and government agencies build a rich history for ongoing analysis by recording and time stamping executed decisions, observable operational and financial outcomes, and environmental variables of particular interest.

3. Monitor actively and richly: In addition to the rich historical data, both direct impacts and reactions from or to decisions are actively monitored, mined and reported upon to key security stakeholders.

4. Model impacts and sensitivities: High performers construct and enhance dynamic, learning models via the continuous stream of active, rich data so as to better understand the relative effectiveness of decisions and the reactions of regulatory and commercial entities.

5. Advocate positions: High performers advocate their positions based upon modeled results through industry associations, shipper forums, regulatory hearings, and state and federal legislators.

6. Document plans, policies and procedures: High-performance organizations further improve the planning process by crafting plans and supporting documents from modeled results, executing the plans, and then recording feedback.

repeat" can engender continuous improvement in security. In this way, they exercise one of the key traits of high performance: High-performance businesses are committed to consistent improvement, not continual drastic change.

Advocacy also is vital. Whether it is through regulatory, legislative, equity, media or partner channels, all affected organizations should work to influence the direction of future security efforts. For example, shipper associations that called attention to congestion at the ports of Los Angeles and Long Beach helped convince American and Mexican governments to let intermodal freight travel in-bond into the United States from Manzanillo and Lazaro Cardenas, without incurring extra security-driven delays. In another instance, 51 mayors petitioned the DOT and DHS in January 2005, requesting operators notify municipalities when freight trains carry hazardous materials through their towns. These actions opened the door to important legislation, such as Senator Joseph Biden's Hazardous Materials Vulnerability Reduction Act of 2005, which is intended to regulate potentially dangerous shipments on a national level.

No organization should expect its first- or even second-generation security models will be so successful to the point where future enhancements are unnecessary.

This is why closed-loop planning is so important: It helps ensure feedback is immediate, insightful, actionable and meaningful. By tactfully advocating an organization's position through the right channels, organizations help themselves and provide an important service to policymakers who struggle to stay informed on all issues and understand the business practices and risk points of all organizational models. As evidenced by the controversy surrounding DP World's attempted acquisition of Peninsular & Oriental Steam Navigation's (P&O) American port operations, simply recognizing the implications of public policy is a daunting challenge.

Proceeding in a clouded and complicated future

The near certainty of future security "incidents" is hardly comforting. Nor is the likelihood that an increasingly complex and dynamic global security environment will expose most businesses to greater risks and higher costs. A third unsettling dynamic is the rise of more—and more influential—regulatory bodies and the associated political pressure to manipulate business activity. All of these events are sure to complicate organizations' quests for increased growth, efficiency, profitability and, ultimately, shareholder value.

While navigating through an uncertain future clouded with more and complex regulations may seem daunting, organizations can help ensure their success by developing and implementing an optimal security model—one that features an innovative "sense and respond" capability and the capacity for continuous improvement and insightful outreach. Furthermore, leading executives know rapid change and elevated risk can actually mean new opportunities for higher profits and increased competitive advantage.

By adopting innovative approaches to freight security, they can prepare themselves to maximize growth opportunities and accelerate their journey to high performance.

About the author

Jade Rodysill is a senior manager in the Accenture Supply Chain Management service line who helps clients across industries improve their performance through innovative supply chain strategy solutions. He is an expert in freight security and logistics, and frequently speaks with the media on a broad range of supply chain issues. He holds an MBA from The Wharton School of the University of Pennsylvania.

In addition to sponsoring Texas Christian University's Supply and Value Chain Center, he is a member of the Council of Supply Chain Management Professionals (CSCMP) and a board member of its North Texas Roundtable. He also serves on the North Texas Commission's Logistics Committee, where he sits on the regulatory and security subcommittee. Based in Dallas, he can be reached at jade.rodysill@accenture.com.

About Accenture Supply Chain Management

The Accenture Supply Chain Management service line works with clients across a broad range of industries to develop and execute operational strategies that enable profitable growth in new and existing markets. Committed to helping clients achieve high performance through supply chain mastery, we combine global industry expertise and skills in supply chain strategy, sourcing and procurement, supply chain planning, manufacturing and design, fulfillment, and service management to help organizations transform their supply chain capabilities. We collaborate with clients to implement innovative consulting and outsourcing solutions that align operating models to support business strategies, optimize global operations, enable profitable product launches, and enhance the skills and capabilities of the supply chain workforce. For more information, visit www.accenture.com/supplychain.

About Accenture

Accenture is a global management consulting, technology services and outsourcing company. Committed to delivering innovation, Accenture collaborates with its clients to help them become high-performance businesses and governments. With deep industry and business process expertise, broad global resources and a proven track record, Accenture can mobilize the right people, skills and technologies to help clients improve their performance. With more than 129,000 people in 48 countries, the company generated net revenues of US$15.55 billion for the fiscal year ended August 31, 2005. Its home page is www.accenture.com.