Massachusetts Institute of Technology

June/July 2007 // Volume 3 // Number 5

supply chain strategy

A newsletter from the MIT Center for Transportation & Logistics

How Risk Management Can Secure Your Business Future

BY JAMES B. RICE, JR. AND WILLIAM TENNEY

When U.S. Customs and Border Protection issued new Customs-Trade Partnership Against Terrorism (C-TPAT) security criteria for importers in March 2005, many companies worked aggressively to gain compliance. Soon they asked, "are we finally secure and ready to respond to disruptions?" As it turns out, this is the wrong question.

Too often executives define security and risk management in terms of only physical asset protection or guarding against unlikely disruptions, instead of recognizing that both are central to protecting the firm's economic viability. As a result, most companies miss opportunities to increase their competitiveness and are vulnerable to dramatic business failures.

A few pioneering firms have adopted a more enlightened approach to security and risk management. Learning from them, and synthesizing the work done at Target and the MIT Center for Transportation & Logistics, we have developed a supply chain risk management maturity model that instead focuses on protecting — i.e., actually maintaining — the firm's economic viability that may be used as a strategic road map.

The case for economic viability

Security in the U.S. is frequently associated with the 9/11 terrorist attacks. However, while the attacks were tragic, they impacted a relatively small number of firms: mainly those in impact zones or highly dependent on just-in-time imports. Consequently, many companies don't recognize that such incidents endanger their economic well-being, and fail to protect their businesses from security breaches and supply chain disruptions. Unfortunately, the aggregate of these risk-exposed firms makes the entire import supply chain less secure and more vulnerable.

Yet there are a number of key reasons that make the case for protecting the economic viability of risk-exposed supply chains.

Compliance: Governments, the U.S. in particular, have attempted to reduce national vulnerabilities through various voluntary and regulatory requirements and programs for freight system security (e.g., C-TPAT). These initiatives offer benefits such as reduced inspections and faster border crossings in return for guaranteeing enhanced security within their supply chain. These benefits are not yet fully delivered, but they are significant and offer potential competitive advantages for companies that make the effort to comply.

Reduced Losses: For some companies the threat of financial loss provides motivation to make supply chains secure. In 2003, Intel lost $10 million worth of Pentium 4

continued on page 2

INSIDE

chips when a van carrying the product was stolen at Heathrow Airport. In late 2002 Cisco lost $3 million worth of routers when a truck was broken into in Santa Clara and the contents stolen. These are but two of the more than $60-75 billion cargo losses estimated each year.

Resilience: The destruction wrought by Hurricanes Katrina and Rita underlines why firms must manage corporate risk by developing business continuity plans for disruptions. Ultimately, the most significant risk to each business — and to a country's economy and livelihood — is the risk of catastrophic business failure. The economic cost of such calamities can be staggering; even the fully expected U.S. West Coast Port lockout in October 2002 cost an estimated $20 billion. The impact from full system-wide disruptions will likely be higher. In a simulated Port Security War Game conducted by Booz Allen Hamilton in 2002, the estimated impact on the U.S. economy totaled $58 billion, with an estimated 52-day backlog at U.S. ports. Admittedly this is a worst case scenario; even so, waiting 52 days for your product could mean "game-over" for those companies that fail to prepare and protect.

Brand Protection: The seven charter members of C-TPAT — Ford, General Motors, Daimler-Chrysler, Target, Sara Lee, Motorola and BP America — share a common interest: to protect invaluable brands. For these organizations a crucial reason for managing supply chain risk is to protect and even enhance the company's brand and reputation. This includes protecting against the rampant counterfeiting of branded products. Fake products can cause injury and even fatalities, expose organizations to product liability claims, and harm the image of their brands.

Even when high-profile companies such as retailers are not moved by the threat of cargo losses through theft (the value of their containerized merchandise is relatively low and insurable), they are concerned about protecting their brand. For these enterprises, the real risks are less about something being removed from their supply chain and more about something being introduced into their supply chain. Imagine the impact if one of their containers was found to contain narcotics or illegal immigrants. Even if they were able to escape the media scrutiny, they would lose their C-TPAT benefits resulting in more inspections and higher inspection and inventory costs.

[Key Takeaways]

- Supply chain security is more than fencing off assets or avoiding disruptions; it should be part of your organization's DNA. Embedding security in this way strengthens the company and safeguards its economic future
- There is no standard blueprint for attaining the highest levels of supply chain security. However, some market leaders have created pathways to the top that others can follow

As these scenarios demonstrate, the risk of serious disruptions to individual companies and even economies is stultifying — and it is only a matter of time before your organization is impacted to some degree. Security must include securing the future of the firm by enabling it to continue to maintain its economic activities in crisis situations.

Follow the cow path

How do firms protect their economic viability? Our studies suggest that there is a traditional path from non-compliant (vulnerable and exposed) to risk-managed, secure and resilient. There are many variants of the pathway, but we believe that a select group of pioneering companies has blazed a trail that other organizations should consider as they plan their own routes (see Supply Chain Risk Management Maturity Levels page 3).

In the same way that the streets of Boston basically fol-

supply chain strategy

Editor: Ken Cottrill
Associate Editor: Anne Saita
Publisher: Jennifer O'Grady
Advisers: Yossi Sheffi, Professor of Engineering Systems and of Civil and Environmental Engineering at MIT, and CTL research staff

LARSTAN BUSINESS REPORTS

Editorial
Chief Executive Officer: Larry Genkin
Editorial Director: Anne Saita
Circulation & Fulfillment Manager: Stan Genkin
Art Director: Rob Hudgins
www.larstan.com
Larstan Business Reports is an independent news agency headquartered in Washington, DC. Larstan's editorial services include: newsletters, book publishing, white papers, market research and media syndication.

Articles in this journal draw on a variety of sources, including published reports, interviews with practicing managers and consultants, and research by management scholars, some but not all of whom are affiliated with Larstan Business Reports, MIT and the Center for Transportation and Logistics. Articles reflect the views of the author.

MIT Center for Transportation & Logistics

The MIT Center for Transportation & Logistics (CTL) is a world leader in supply chain management education and research, ranking consistently as number one. CTL contributes to the academic knowledge in the field and helps companies gain competitive advantage from its cutting edge research. The Center's graduates occupy senior supply chain management positions in almost every industry and continue to use the Center's resources to update their knowledge and skills. Web: http://ctl.mit.edu. Tel: 617-253-5320.

Subscription Information
Subscription price is U.S. $295 (10 issues); single copy: U.S. $37.50. To subscribe to Supply Chain Strategy, call 800-890-6263 for US and 914-962-6292 for outside the US.
Web: www.MITsupplychainstrategy.com

Letters and Reader Feedback
Letters, editorials, ideas for articles, and other contributions may be submitted to Ken Cottrill, editor, at SupplyChainEditor@larstan.net.

Services, Permissions, and Back Issues
Supply Chain Strategy is published 10 times a year by Larstan Business Reports at 209 Canterbury Court, Blue Bell, PA 19422. POSTMASTER: Send address changes to Supply Chain Strategy, PO Box 23, Shrub Oak, NY 10588. To resolve subscription service problems, please call **800-890-6263 for US and 914-962-6292 for outside the US.**

Mapping by level of progress and key process area

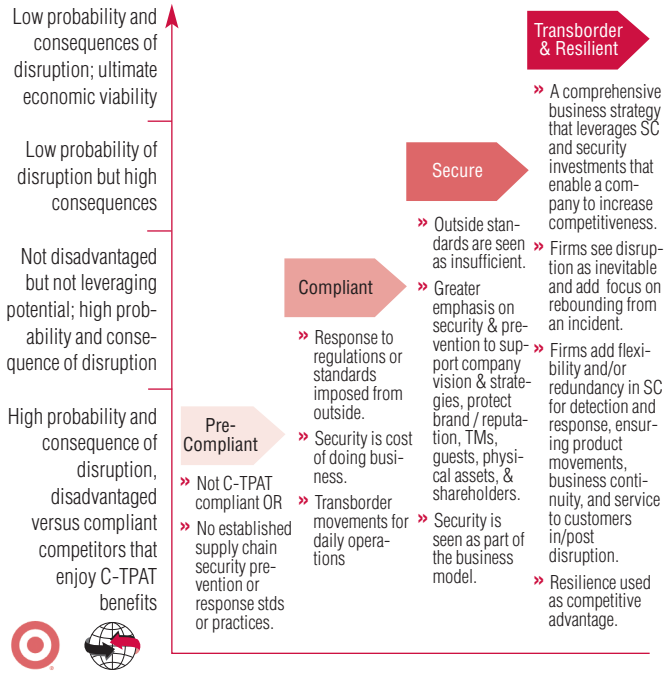
Key Process Areas and Focus	Level 1 Pre-Compliant	Level 2 Compliant	Level 3 Secure	Level 4 Resilient
Leadership	» No risk focus	» Program compliance	» Prevention, security	» Response for advantage
Internal Integration	» None	» Reactive coordination	» Proactive coordination	» Integrated teams manage security, resilience, risk
External Partnership	» No defined partners	» Limited interaction	» Partners involved in security only	» Partners in risk management, resilience
Visibility	» Limited to no visibility	» Some system visibility	» Partner visibility	» End-to-end visibility
Risk Management	» No standards	» Nascent security standards	» Partners pre-screened	» Partners help manage risk
Risk Detection	» None	» Some reactive procedures	» Some proactive procedures	» Procedures to ID emerging risks
Training	» No training	» Internal training	» Security training for vendors	» Full scenario & contingency exercises
Communication	» No plans	» Reactive	» Proactive	» Response and recovery plans
Culture	» No awareness	» Compliance only	» Security and compliance	» Actions affecting security, resilience

lowed the old cow paths that weaved in and out of the city's hills, so too can companies model their approach after the leaders that have progressed from pre-compliant to compliant, secure and resilient supply chains to protect economic viability.

Beware — following the path will not guarantee C-TPAT compliance. Also, it ought to be considered more of a journey than a destination. The leaders do not limit their view to incremental improvement or cost containment, but instead recognize compliance and security as part of a way to enhance the broader competitiveness of the firm.

Consider also the ramifications outside your organization. It's not enough to focus internally as companies must understand the public relations implications of their actions and the actions of other enterprises in their industry. Within Target, for example, the interconnectedness of the country's trade industry is clearly recognized. Put another way: "If something blows up inside a Target container, it would be really bad. But if something blows up inside a Wal-Mart container, it's still really bad," relates the approach taken at Target.

Supply Chain Risk Management Maturity Levels



The pathway – definitions of maturity levels

As suggested our respective research has revealed a common path with four stages to achieving economic viability. While this is not a definitive model, it does provide a basic road map that can be used to assess your current position and help you progress towards higher levels of security and resilience.

Level 1 — Pre-compliant: Pre-compliant companies are not yet meeting C-TPAT security or other compliance criteria, or have no established supply chain security prevention or response standards or practices. In some cases, limited prevention measures such as personnel checks and freight protection practices are in place. The firm's economic viability is at risk. The probability of a business disruption is high, as is the likely impact, and these firms are less competitive than their C-TPAT-compliant rivals.

Level 2 — Compliant: C-TPAT-compliant companies carry out security or other mitigation measures as a response to externally imposed regulations. Aside from being compliant, companies at this level are primarily reactive, and see security as a cost of doing business. There is a lower risk of compliance violation, but still high probability and impact of disruptions. These firms may enjoy C-TPAT benefits of lower inspections and shorter border delays, but they are not leveraging their security investment.

Level 3 — Secure: Secure companies see externally imposed security standards as inadequate, and have instituted a more rigorous approach to protect the brand, employees, physical assets and shareholders. At this level the focus is on preventing a disruption from occurring. Security is seen as part of the business model. These firms

LOOK FOR A MESSAGE

Our research indicates that there are several "enlightened" firms that are leveraging their security operations to protect the firm's economic viability and in some cases, help create competitive advantage. These include Intel, Target, IBM, UPS, Nike, Maersk and APL. One hint as to how progressive a firm is in this sense can be found in stated objectives of the security operations – do the goals focus on asset protection or serve the corporate strategy and objectives (i.e. serve customers)? Target Corporation's stated supply chain security objectives provide a good example of how such considerations play a critical role in serving the organization's corporate goals – and ultimately its guests.

Target Supply Chain Security Operation's Objectives

1. Safeguard Target's direct import strategy
   a. Support speed to market, be in stock
   b. Rebound from disruption
2. Protect the brand and assets
   a. Prevent infiltration by terrorist or criminal groups
3. Ensure regulatory compliance
   a. Meet C-TPAT criteria

As these objectives suggest, Target seeks to deliver business value through its security operations by paying attention to ensuring that product is available, and by protecting its brand image, with C-TPAT compliance as a supporting goal and a means to achieve these ends. In this case security is effectively managing risk to protect economic viability. We consider this to be "Big 'S' Security" because security's role is big. Most companies however, are not so progressive and are in need of some guidance to find their way to leverage security. In these firms managers must show how security functions support the firm's core business; they must integrate security into the decision-making process and business operations.

are leveraging their C-TPAT investments and are working with suppliers and customers to understand the system risks and vulnerabilities. However, the impact of a disruption is still high.

Level 4 — Resilient: Resilient companies see risk management as an element of a business strategy that changes the way the enterprise operates and increases competitiveness. Recognizing that disruptions are not entirely preventable leads to additional focus on rebounding quickly from incidents. The company adds flexibility and, where necessary, redundancy in the supply chain to detect and respond proactively to potential risks and crises. These firms have reduced their risk of non-compliance, are less prone to security breaches and have mitigated the consequences of disruptions. They are leveraging their security investments, and security plays an integral role in serving the business purpose. As such, these firms have prepared themselves for ultimate economic viability.

Plotting your route

There is no standard pathway to security and resilience and companies have to make trade-offs to arrive at the path that best suits them. The choice depends on many factors including business strategy, cost structure and the type of industry. Enterprises might have to make a choice between security and resilience investments, for instance when a security initiative to protect information hinders a resilience initiative to create flexibility via supplier collaboration. Despite this path uncertainty, we have observed some common capabilities that leaders have which practitioners can consider in mapping their own path:

- Internal Integration of planning and operations, and response coordination of logistics, sourcing, government affairs, compliance, security and legal.
- External Partnerships with business-critical external stakeholders such as vendors/factories, ocean carriers and all cargo handlers
- Risk Management that is exercised via standards to all supply chain business partners, identifying and assessing threats and vulnerabilities
- Risk Detection systems for "early warning" of potential or actual supply chain disruption
- Education and Training — education for awareness and training for response
- Pre-event Communication protocols for sharing business-relevant supply chain information among internal and external partners
- Security and resilience culture that permeates the firm and recognizes risks as well as key design choices that affect both security and resilience

The maturity model is by no means the final word on supply chain security, but a starting point in an ongoing conversation with other importers. It is only through this type of synthesis that companies, economies and countries will develop the necessary resiliency to rebound from the next disruption. ◆

James B. Rice, Jr. is director of the MIT Integrated Supply Chain Management Program. He can be contacted at jrice@mit.edu. **William Tenney** is Group Manager, Business Intelligence and International SC Security at Target Corporation. He can be reached at William.Tenney@target.com.

Reprint #P0706A