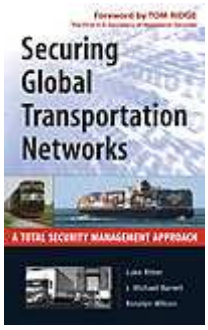
Securing Global Transportation Networks: A Total Security Management Approach

Posted: February 1, 2007



With the dangers of disruption so real, the best precaution is to defend the entire value chain.

On any given day transportation assets in the United States move approximately eight million truckloads of freight across four million miles of highway; 1.5 million railcars traverse over 170,000 miles of track; 2400 flights pass through about 400 airports; and roughly 325 seaports transfer more than 25,000 containers. This translates to responsibility for more than $1.4 trillion worth of goods and nine million cargo containers entering the U.S. alone; global figures are exponentially higher.

However, there is an inherent fragility to this global transportation system, and the economic impact of a significant and prolonged systemic disruption of the global transportation network and the supply chains it sustains would be measured in the billions, if not trillions, of dollars.

Although portions of the global transportation network have been heavily scrutinized in the five years since the terrorist attacks of 9/11 and a host of government and regulatory measures have been enacted, the fact remains that nearly all experts and analysts agree that the global transportation system remains vulnerable to a significant terrorist event.

To take just one example of the threat, the consulting firm Booz Allen Hamilton hosted a war game for 85 government and private sector transportation practitioners. The intent was to examine the economic destruction of a container bearing a dirty bomb being detonated in a U.S. port facility. Following the simulated detonation of the dirty bomb, the war game's decision makers recommended the government shut down every port in the United States for eight days, and some ports for twelve days. Analysis later determined that it would take up to three months to clear the shipping backlog from such an event and, even with these relatively short port closures, the estimated cost to U.S. businesses alone would exceed $58 billion. This figure includes spoilage, lost sales/contracts, and manufacturing slowdowns, but does not account for the longer-term cascading global costs or the toll on the U.S. or foreign governments.

Natural events can also cause major disruptions, such as in August 2005 when Hurricane Katrina closed U.S. ports in the Gulf Coast region and destroyed or disabled other critical transportation infrastructure in Texas, Louisiana, Alabama, and Mississippi. Indeed, with the ports and the transportation routes they serve closed for several weeks and degraded for many months, post-Katrina analysis showed total waterborne exports to the region fell $1.2 billion during September versus the previous month, led by losses in New Orleans ($649 million) Houston ($540 million) and Gulfport ($126 million), while crude oil imports to the storm-hit region during

September 2005 were down 26 percent compared with September 2004.

Even more worrisome on the natural disaster front is the fact that many public health experts now fear the mutation of the naturally occurring H5N1 'avian flu' virus into a strain that can be transmitted among humans, potentially resulting in another global influenza pandemic like the one in 1918, which killed more than 20 million people.

The challenge

Are terrorism, political upheaval, natural disasters, accidents and other large-scale disruptive events happening more frequently, or are they just having a more significant impact than in previous years? The answer is yes—yes more disruptions are occurring and yes these disruptions are having a more significant impact. The primary reasons are three-fold:

The impact of globalization and the attendant competitive forces of the global free market, which dictate that business processes be carried out by the lowest-priced provider wherever they may be located, increases the complexity and diversity of a firm's Value Chain.

The dramatic and growing interconnectedness and mutual dependencies of global critical infrastructures such as ports, highways, railroads, airports, telecommunications links, and power plants, coupled with the advent of lean business processes that minimize standing inventories, and in turn create increased collective risk from what would once have been relatively minor disruptions.

The continual threat of discontinuous events posed to this globalized and interconnected world by events that can severely disrupt normal patterns and cause changes in the free flow of goods including, but not limited to, severe weather, political upheaval, labor disputes and terrorist attacks.

As an outgrowth of the interplay among these three factors, today's adverse events occur more often and in turn are more likely to have wider-ranging cascading effects because of them. Furthermore, with the increased likelihood comes increased severity. This phenomenon is the result of what noted enterprise vulnerability and business resiliency expert Yossi Sheffi calls the high frequency of rare events, explaining that, "while the likelihood for any one event that would have an impact on any one facility or supplier is small, the collective chance that some part of the supply chain will face some type of disruption is high." With each piece of the global transportation network increasingly tied to every other part, the cascading impacts from adverse events can now extend further than ever before.

In addition, some of the most pressing challenges to conducting efficient global trade might come not from the event itself, but from the response of the affected governments. The evidence from 9/11 indicates that the U.S. government's first response will likely be to try and halt means of further attack or cross-contamination by shutting down the affected transportation links. It stands to reason that other governments around the world would choose to do the same. The key players in the

global transportation network need to develop a way to get ahead of this problem and to circumvent the threat by instituting new and improved security practices.

The solution: Total Security Management

What is the solution for firms faced with such pervasive and potentially existential risk to their business operations? The best approach is to work through a framework that integrates security prerogatives across all the activities of the enterprise. Doing so creates opportunities to create value in new and significant ways that include everything from cost savings from improved business processes and reduced theft from better asset management to enhanced brand equity or improved preparedness for catastrophic loss. In this manner, security can be turned from a net cost into a net benefit.

Total Security Management (TSM) is a broad-based framework focusing on developing and implementing comprehensive risk management and security 'best practices' for a firm's entire Value Chain. It works with and through key internal and external stakeholders to ensure the use of a comprehensive approach to securing fixed assets, assets in transit, brand equity/goodwill, and human capital. It also emphasizes business continuity planning and an evaluation of the firm's suppliers, distribution channels, facilities selection criteria, and internal policies and procedures that support preparedness for disruptive events.

The intellectual foundations of the TSM approach draw from the seminal work of W. Edwards Deming and the manufacturing process improvements he championed through "Total Quality Management" (TQM) which, like Total Security, was based on the enterprise-wide application of best practices and measurable value creation.

As with the challenge to re-think manufacturing processes in the 1970s and '80s and make quality an integral part of each of the firm's business activities, the security and business continuity challenges facing today's firms require fresh thinking about how to identify and implement security improvement solutions in a manner consistent with the core business imperative of creating value from all actions and activities. In other words, firms need to find ways to implement security-relevant practices and procedures that also create value, be that value in the form of labor savings, such as when certain automated technologies replace manual processes, or enhanced brand recognition, such as through championing the adoption of new end-to-end Value Chain security practices. The bottom line is that in business security matters and it should be managed to create value.

The scope of TSM

Total Security Management refers to much more than the traditional security concerns of point defenses, security guards, and network passwords. Though these tactical considerations remain important, TSM focuses on security in the broader strategic sense by integrating security and resiliency initiatives into the

decision-making process on everything from vendor and third-party logistics selection to the location of outsourced production lines and call centers. It does so in recognition of the impact that the firm's broad panoply of partners, customers and others can play in overall preparedness for disruptive events.

Specifically, a firm's stakeholders can be defined as those interested and committed parties that interact with or influence an enterprise and its activities. Collective benefit is enabled by implementing a common understanding of the enterprise's goals and those of all its partners, ideally with the objectives and interests overlapping as much as possible. If this development of common objectives can be achieved enhancing and perfecting communication among stakeholders can increase value for an organization and those with whom it does business.

The TSM focus on value creation

The TSM approach was created to offer an all-hazards approach with the potential for appreciable process and efficiency gains that offset the corresponding investment in new and more secure business practices. This approach of using a business case to justify the implementation of TSM is particularly important for it draws out the reality that, at present, there is a marketplace failure in terms of properly rewarding firms that implement security best practices and take a dedicated approach to business continuity and resiliency.

Firms that implement security initiatives that are quantifiably more effective and more comprehensive than those of their competitors should expect to be rewarded accordingly by the marketplace. The critical business process of measuring return on investment for security initiatives can provide valuable data to industry analysts, institutional investors, and insures—all of which influence the firm's market valuation.

By highlighting existing (although often unaccounted for) risks, TSM helps define a firm's risk profile more fully in order to foster better-informed risk management decisions, which in turn help protect the enterprise from surprise.

As for covering the costs of some of the TSM process improvements, some industry studies report that the combined savings in paperwork, manpower and theft reduction will cover most if not all of the costs associated with the new systems. "The investment required to create a more secure supply chain is easily justified when compared to the costs associated with experiencing longer, unpredictable lead-times or acute disruptions. Among other things, these costs come in the form of:

- Additional inventory
- Slowing or shutting down production lines
- Lost revenue due to stock-outs or missed promotions
- Longer cash-to-cash cycles
- Higher insurance rates
- Increased transportation costs (e.g., more expedited shipments)

TSM in action

The specific implementation of Total Security Management will vary from firm to firm and may require examining not only first tier but also second and third tier partners for critical functions; moving from a country or region-specific focus to a global one; and expanding crisis management planning to include business continuity planning as well. The Total Security framework is bounded by Five Strategic Pillars that define its central tenets for all security processes, including that they must:

- Create value for the firm
- Involve all relevant Value Chain partners
- Institute continual improvement
- Help avoid, minimize or survive discontinuous events, and
- Support business continuity plans

These pillars are in turn supported by Four Operational Enablers, which cover important focus areas for improvement including implementation of industry best practices, increased situational awareness, reliance upon training and exercises, and outreach to all relevant parties. In practice, as in the layout of this book, the initial application of the Strategic Pillars and the Operational Enablers is achieved at the tactical level by using the risk management approach to assess operations and processes across four critical functional areas: protection of fixed assets, assets in transit, brand equity/goodwill, and human capital. Relative resiliency and preparedness can then be benchmarked against other firms and process improvements can be analyzed in terms of their relevance to and conformity with the TSM Value Creation Model.

The world is changing all around us and the combined forces of globalization, infrastructure interdependence, and discontinuous events are providing incentives to make global transportation networks more resilient. The tipping point with regards to the need for Total Security has come, but it has come only recently. The timing is right for firms to begin managing security in a concerted and holistic fashion that creates value for the firm and a return on investment from reasonable security practices.