A Framework for Protecting your Supply Chain:

Recent terrorist threats and security incidents have heightened awareness regarding supply chain security. But many managers still underestimate supply chain vulnerability and struggle with where to focus their security efforts. Here is a framework for doing just that.

Increased threats of terrorism require heightened awareness of company and supply chain security. In the past, firms may have considered only the potential threat to their own operations when considering defense protection. However, given the interconnectedness of companies, products, and transportation infrastructure in today's high-speed global supply chains, there is growing concern that disruptions can reach beyond an individual firm, which leads to the need for a broader supply chain defense framework.

As such, today's organizations must proactively enhance their supply chain resiliency against terrorism. They need to enhance overall security as well, to protect customers, the public, and brand equity. This starts with understanding the five key potential adverse consequences of supply chain security failures:

1. A terrorist attack against a firm's supply chain might cause widespread disruption to customer delivery capabilities leading to a loss of short-term revenue and creating a service failure.

2. There could be reduced brand equity if customers believe the attack occurred because of a supply chain security failure resulting from neglect.

3. Loss of revenue could lead to investor discontent with the firm's performance, and the subsequent sale of equity investments.

4. This disruption could also increase regulatory scrutiny.

5. A terrorist attack could result in significant legal liability.

While the above are likely primary consequences for the target firm, secondary consequences extending beyond the target firm including other supply chain partners are also possible. If supply partners perceive the attack was due to the firm's insufficient security efforts, the supply chain relationship would suffer and could potentially be dissolved.

Since supply chains are vulnerable to attack and subsequent security failures, supply chain defense has become an increasingly important issue for practitioners. Unfortunately, a comprehensive framework for securing the supply chain has not yet been created. This article discusses such a framework to guide practitioners in organizing security initiatives.

Defining security

Supply chain management security has been defined as: "The application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism, and to prevent the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain."

This definition implies that effective supply chain security management seeks to prevent supply chain assets from being a target of terrorism or used as a method to facilitate terrorism through effective application of management policies, procedures, and technology. A number of observations can be drawn from this definition. First, supply chain assets are defined as not only the equipment and facilities used to carry out supply chain processes, but also the product, information, and human resources required to operate the supply chain.

Therefore, supply chain protection does not stop with securing a facility through gates and locks. It extends to the protection of products and people involved in supply chain activities, as well as the internal and external information flows across the supply chain. Second, supply chain defense is not simply a matter of ensuring the safety of these assets, but also preventing theft, damage, and unintended intrusions that could disrupt supply chain operations.

the security framework

To create a framework, 10 security competencies are required within and across each firm in the supply chain. Security competencies are created through the development of security capabilities such as infrastructure, processes, assets, and resources that achieve and maintain supply chain security. Security competencies include:

1. Process Strategy: Implementing an effective security environment requires strong executive commitment and a culture that puts a premium on security. Top management needs to encourage frank discussions regarding the importance of security, both for the safety of stakeholders and to maintain the value of the firm's brand. Top management must be visible in their commitment and dedication to implementing security initiatives. Some firms have created a "chief security officer" position to provide additional structure to security initiatives.

2. Process Management: Process management describes the procedures and actions taken to ensure the security of each activity involved with the purchase, manufacturing, and distribution of raw material into a facility and finished product out of a facility. Process management also requires in-depth understanding of firm and supply chain processes in order to identify vulnerabilities that may cause disruptions. Process management includes the use of simulated incidents to test the integrity of procedures and processes.

3. Infrastructure Management: Infrastructure management addresses the manner in which a firm secures its physical premises and products. This includes employee/non-employee access control into facilities (or areas within facilities), employee background checks, empty and loaded trailers security before/during transport, and guards, among other measures. These are the most basic and common methods used to increase security as they serve to form a "perimeter" guarding against unauthorized entry.

4. Communication Management: Firms need to develop strategies to share potential threat and security information internally with employees and provide communication channels for employees to use when a potential threat exists or incident occurs. Threat awareness and security training programs need to be developed in this regard. Similarly, the working environment may need to be changed to identify and challenge unknown personnel in a facility. In this sense, communication management is related to process strategy.

5. Management Technology: Management technology is applied to detect a potential security threat or incident and to share timely and reliable information internally and externally. Information systems provide a first-defense mechanism to understand trends in product contamination and missing shipments, as well as to identify the root causes of these occurrences. These information systems are also critical in obtaining and sharing information with suppliers, customers, third party service providers, and government agencies to identify potential problems or recovery actions at the intersection between firms.

6. Process Technology: Process technology is the presence, use, and ability of information systems to track product movement and monitor processes internally and across the supply chain. Process technologies include the use of tracking technologies, such as RFID and smart-seals, and process improvements. Many firms have not progressed beyond implementation of physical security measures (gates, guards, and cameras) and thus have yet to gain the potential advantages that may come from tracking technologies.

7. Metrics: Security metrics involve the continuous development, testing, application, and redefinition of guidelines measuring security-related procedures, plans, and capabilities. Metrics might be implemented to comply with specific guidelines, such as those of a customer or government agency, or the metrics may be developed and captured by the firm to assure adherence to security guidelines. Similarly, a firm may conduct audits or have an external entity certify that current procedures and processes are in place to increase security.

8. Relationship Management and 9. Service Provider Collaboration Management: These competencies are critical to the discussion of supply chain security. The reason: a company cannot create a supply chain protection program alone; it must work collaboratively with other supply chain partners. Collaboration with external entities (customers/suppliers and service providers) is necessary to ensure that security procedures are communicated and followed. Global relationships present added security difficulties as the target firms are often unable to monitor these partners and protect against theft, contamination, or insertion of unauthorized counterfeit cargo.

10. Public Interface Management: Public interface management describes the security-related relationships and exchanges of information with the government and the public. Forging relationships with U.S. government agencies is a critical corporate capability to protect against terrorist acts. Firms may actively participate in the development of government standards or security initiatives.

Getting started

The logical question for supply chain practitioners is how to get started along this security framework. As a part of this research completed under the sponsorship of the U.S. Department of Homeland Security, the research team developed a spreadsheet benchmarking tool that is available online, at no cost, to allow firms to compare their practices both internally across their organization and divisions as well as to benchmark their practices against organizations demonstrating high security performance. The spreadsheet and the food research summary are available at http://www.bus.msu.edu/msc/SCMExecBrief/.

The spreadsheet provides a framework and a tool to allow a firm to complete both an internal assessment and an external benchmark. The internal assessment begins when individuals representing multiple functions and divisions within the firm complete the questionnaire. The questionnaire asks each individual to assess their firm's emphasis on the security initiatives contained in the framework.

The spreadsheet then summarizes the perceptions of the multiple respondents by providing a minimum, mean, and maximum score. A review of the minimum, mean, and maximum score for each initiative and competency can stimulate substantial discussion regarding the consistency of perceptions across functions and divisions. The discussion is useful to synthesize a common perception regarding security initiatives that enhance the firm's ability to develop a common direction for enhancing security capabilities.

It is possible that supply chain security is nothing more than good business. It's hard to argue that firms should not hire trustworthy employees, lock their doors, share relevant information both internally and externally, track inventory, and protect their product and assets to ensure firms' long-term viability and the safety of their customers. Firms should use the framework presented here to build a security culture into their strategic and operational objectives-not just when it is legislated or required by customers, but because doing so stands to benefit all parties involved, particularly end consumers.

Author's note: This research was supported by the U.S. Department of Homeland Security (Grant number N-00014-04-1-0659), through a grant awarded to the National Center for Food Protection and Defense at the [University of Minnesota](http://search.proquest.com.ezproxy.trident.edu:2048/docview/197209740?pq-origsite=summon). Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not represent the policy or position of the Department of Homeland Security.