

## Global Supply Chain News: A New Framework for Supply Chain Security

### Need for Improvement is Well Understood, but How Can Companies Develop an Integrated Approach?

#### SCDigest Editorial Staff

From both a governmental and private company perspective, attention to supply chain security obviously has risen dramatically since the terrorist attacks of Sept. 11, 2001, especially with regards to potential terrorism threats.

In reality, of course, there has always been attention paid to supply chain security, but before Sept. 11 the focus was primarily on potential theft and related crime.

Now, companies have to worry about both the terrorism threat, in which their supply chains may be used to convey terrorist materials or launch a terrorist attack, as well as to protect against increasingly rampant and violent crime across the globe.

**Andreas Wieland**, a research associate at the Competence Center for International Logistics Networks at Germany's Technische Universität Berlin, notes in a recent article in *The Journal of Homeland Security* that "Though many companies still consider supply chain security to be just cumbersome requirements imposed by legislation, other companies recognize that the provision of supply chain security can be a step toward customer orientation and thus a competitive advantage."

He also says that in many ways, improving supply chain security should be thought of as another component of overall quality management – a connection many companies have not yet made. (To read the full article, go to: [Strategic Supply Chain Security](#).)

But even for those companies focused heavily on supply chain security, it is difficult to know where to

***Improving supply chain security should be thought of as another component of overall quality management – a connection many companies have not yet made.***

---

begin, and also to think about the problems and solutions holistically and in an integrated fashion.

Wieland says companies need better supply chain security models to achieve that more integrated approach, and offers a six-level framework that can help companies get there.

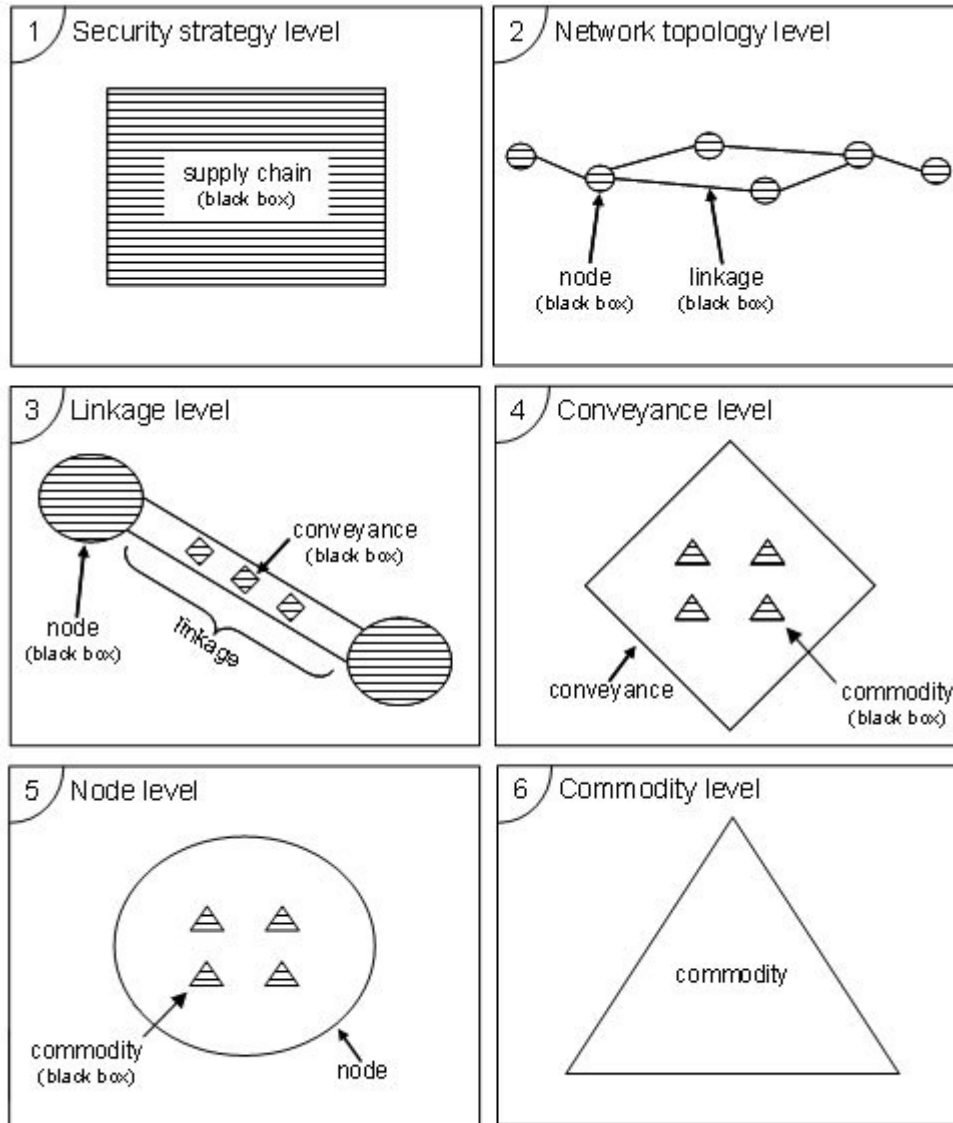
#### **It Starts with Strategy and Network Design**

Weiland's framework consists of six integrated levels:

1. **Security strategy:** First, a general security strategy for the entire supply chain is developed, and an overall guiding framework for cost-benefit analysis is established.
2. **Network topology:** Security is actively considered in overall network design, and the precise network is defined and documented so that all components of it can be considered in secu-

**Global Supply Chain News: A New Framework for Supply Chain Security (Con't)**

**Supply Chain Security Framework**



Source: Andreas Wieland, Journal of Homeland Security

rity processes and programs. This is also the level where risk mitigation through network redundancy or contingency plans can be considered.

3. **Linkages:** Considers how nodes in the network are connected in the physical move-

ment of product. Security measures for each route are analyzed and developed. Hand-offs at each node are especially important.

4. **Conveyance:** Case-based security measures have to be configured for each "conveyance," or transporta-

## Global Supply Chain News: A New Framework for Supply Chain Security (Con't)

tion component – such as specific types of trucks or containers. This needs to be considered in conjunction with the type of commodity being handled (see below).

5. **Nodes:** Each node within the network, such as a factory, distribution center, or port terminal, needs to be considered and appropriate security measures put in place.
6. **Commodities:** Finally, a company needs to consider the specific characteristics and requirements for each commodity or product that is managed by the supply chain.

While most companies understand the need for better supply chain security and are taking active measures to improve what they have in place, “no effective system can be found that acts as a superstructure to join operational security measures and directs [companies] to a superior [supply chain security] strategy,” Wieland concludes.

Using this model, companies can segment their supply chain security strategies into manageable parts, and develop preferred degrees of security for each link, node and product category.