

SUPPLY CHAIN SECURITY WITHOUT TEARS

By Hau L. Lee and Michael Wolfe

Supply chain managers today face a dilemma: How do you improve security without jeopardizing supply chain effectiveness? The answer may lie in the principles of the quality movement. Total quality management taught us that we can decrease defects without increasing costs – or achieve “quality without tears.” By applying these lessons, we may be able to create strategies that both prevent and mitigate security breaches while also strengthening productivity.



Prior to Sept. 11, 2001, most discussions of freight transportation security focused on controlling theft and reducing contraband such as drugs, illegal immigrants, and the export of stolen cars and construction equipment. After Sept. 11, the highest-order definition of freight security changed from theft-proof to tamperproof. Terrorism and the threat of weapons of mass destruction have transformed perceptions of security across the supply chain. Suddenly, intermodal containers have become potential weapon delivery systems—a poor man’s missile. Weapons delivered by such means would put at risk large numbers of lives, significant infrastructure, public and business confidence, trade, and prosperity.

Government and business leaders now are searching for ways to prevent terrorist attacks on or through our freight distribution systems. At the same time, questions have been raised within the supply chain profession as to whether existing best practices remain sound. There is no doubt that significant changes need to be made—and that these changes will have a significant cost. Both private and public leaders, however, appreciate the need to keep commerce active and vigorous while increasing security.



Hau L. Lee is Thoma Professor of Operations, Information, and Technology at Stanford University. Michael Wolfe is principal of the North River Consulting Group.

ROMA KARRAS



The goal of this article is to help those leaders succeed in this dual objective. We believe that the right strategies and tactics can reduce security risks while, at the same time, contributing to supply chain productivity and effectiveness. One of the most effective strategies may be to apply the lessons of successful quality improvement programs. By doing this, we aspire to (to paraphrase the title of quality guru, Philip B. Crosby's best seller) "supply chain security without tears."¹

Lessons From the Quality Revolution

The quality movement of the 1970s and 1980s provides an instructive model for public and private business leaders as they develop a response to the supply chain security challenge. The quality movement started with the recognition that defects can be very costly to a company. Product failures out in the field can cause a wide range of "external failure costs"—such as customer process down time, increased liability, product recalls, field repair, goodwill damages, adverse effects to future sales, and even catastrophic effects on society. These costs can be far greater than the product cost itself.

This realization provided the strongest motivation for industry to become engaged in "total quality management,"² a process whereby the entire organization, its suppliers, and, in some cases, customers work zealously to improve quality. In a similar manner, companies need to recognize the importance and significant cost of security problems and to engage all stakeholders in driving out security breaches.

The following principles that shaped the quality movement can help frame our responses to the supply chain security challenge.

1. Quality assurance through final product inspection is the last resort. Inspection does not improve quality. Screening is expensive, and it is susceptible to two kinds of statistical errors known as Type I (labeling a conforming item as nonconforming) and Type II (missing a nonconforming item).

2. Assuring that the process is functioning in an in-control state is preferable to final product inspection. A process that is out-of-control will produce many more nonconforming items. Detecting the out-of-control state, identifying the causes, and restoring the process to an in-control state in a timely fashion will always improve quality.

3. Quality assurance requires total organizational focus. Everyone should be aware of the quality imperative. Quality is not just the responsibility of the quality control department or quality inspectors.

4. Prevention is always the preferred strategy. Companies should strive to install processes that ensure nonconforming items cannot be made or, if they are made, that can immediately identify and correct them before they turn into defects.

5. Quality should be designed in. Products need to be designed so that they are less likely to be produced with defects. Processes must be designed so that the process variation is at a minimum.

As these principles indicate, the quality movement has evolved from a focus on inspection to a focus on prevention. Prevention emphasizes education, organizational collabora-

tion, design improvement, process variation reduction, and the accountability of the total company. Crosby argues that an investment in prevention pays off handsomely because it drastically reduces the cost of inspection and the number of product failures. Indeed, many companies have found that it is possible to improve quality without increasing costs or jeopardizing productivity.

We can learn from the quality movement and begin to think about supply chain security more in terms of prevention, process control, and design improvements that will restore supply chain confidence while increasing productivity and reducing costs. Exhibit 1 demonstrates how key aspects of the quality movement can be applied to supply chain security initiatives.

A Win-Win Template

To accomplish this quality-inspired vision of security, we need to identify and promote security measures that also increase supply chain efficiency. Put another way, we must pursue preventative measures that meet the requirements of the win/win template set forth below. The template rests on the critical goals of two communities as they intersect with one another; that is, what security officials want from supply chain managers and *vice versa*. Weaving those views together produces a qualitative template—a conceptual model—to help design and evaluate improvements.³ Embedded within this template are many of the core principles of the quality movement, such as process control and a focus on prevention over inspection.

The template has two perspectives—a security perspective and a supply chain perspective.

Security Perspective. To create a secure freight system, security managers have *three immutable requirements* for supply chain processes and managers.

1. Assure the integrity of conveyance loading, documentation, and sealing.

2. Reduce significantly the risk of tampering in transit—ultimately with comprehensive monitoring for tampering and intrusion.

EXHIBIT 1	
Supply Chain Security and Quality	
Quality Movement	Security Initiatives
Defects are very costly	Security gaps create big risks
Total quality management	Involvement of all stakeholders
Emphasis on prevention	C-TPAP, sealing and anti-tamper technologies
Source Inspection	CSI and source inspection
Process control	Automated chain of custody
Identify, track, and improve quality	Container tracking and total visibility
Root cause analysis	Profiling system for shipments, shippers, carriers, trade routes
"Quality is free"	Higher productivity with supply chain security and confidence

3. Provide accurate, complete, and protected information about shipments to those who need it in a timely manner.

Supply Chain Perspective. Supply chain managers, in turn, require these *four critical items* from security processes and managers:

1. Commit to processing and inspecting qualifying shipments in ways that permit highly reliable and predictable processing times for those companies that adhere to the best security practices and standards.

2. Protect all commercial information given to authorities; this includes protection from Freedom-of-Information and tort disclosure.

3. Harmonize and standardize security processes internationally and domestically.

4. Create security and anti-tampering practices that are by-products of excellent supply chain management practices and are not nonvalue-added activities.

A theme that cuts across the template is better visibility and control through all supply chain processes and activities. These seven requirements can be used to assess the effectiveness of potential supply chain security measures.

Applying the Quality and Win-Win Principles

In the aftermath of Sept. 11, some in government called for heightened inspection of cargoes, containers, and transportation vehicles at ports and border crossings. A group of influential legislators suggested, for example, increasing the inspection rate of containers from the present 1-2 percent to 10 percent. There were even calls for universal inspection of import containers.

If we apply the principles of the quality movement and the win-win template, we see that such solutions would be less than elegant. In addition to the raw costs of higher inspection rates, this approach would have three deleterious effects. First, congestion at the terminals would increase, thereby reducing productivity for terminal operators and transportation companies. Second, the inspections and congestion would slow cargo flows, extend delivery times, and decrease shipment reliability. All of these factors increase inventory costs and reduce service levels for cargo owners and their customers. Third, the security value of the inspections would be offset by the risk that landed containers could hold weapons of mass destruction as they await inspection. Thus, an emphasis on inspection falls short on most of the four critical items of the supply chain perspective and the three security requirements.

We can reduce the number of inspections, our need for inspections, and the negative effects of remaining inspections. The key is to apply the prevention and process control concepts from the quality movement. Happily, some government security initiatives are moving in this direction. The best known are the Customs-Trade Partnership Against

Terrorism (C-TPAT) and the Container Security Initiative (CSI), which are discussed in detail below.

Prevention at the Source

In manufacturing, the way to eliminate inspections is to design and build in quality from the start. For supply chain security, the analogy is to design and apply processes that prevent tampering with a container *before, during, and after* the loading process.

The first “immutable requirement” under the security perspective in the win/win template—“assure the integrity of conveyance loading, documentation, and sealing”—deals with *before and during* the loading process. To meet this require-



We need to identify and promote security measures that also increase supply chain efficiency.

ment, companies can begin by thoroughly vetting cargo-handling personnel and controlling access to plants and warehouses. They also can closely monitor the flow of inbound materials and components, the pick-and-pack process, the staging of outbound loads, and the loading or stuffing process itself. It's necessary to document not only the goods being shipped but also the process of assembling the load. Best practices would include recording the identities of pickers, packers, loaders, checkers, and seal appliers. The quality of shipment-related documentation can be a litmus test for the quality—and attention to security—of the materials handling processes.

The C-TPAT program developed by U.S. Customs is targeted directly at this area. It is a quality-like program open to manufacturers, importers, carriers, and third parties. Applicants begin by completing detailed questionnaires and self-appraisals of their supply chain security practices. Although C-TPAT members manage their own processes, Customs reviews the self-appraisals, visits facilities, asks for modifications if necessary, and reserves the right to perform unannounced verification visits (which C-TPAT leaders insist are not audits). In turn, Customs will provide faster processing at ports and border crossings for C-TPAT participants. The agency also will identify member firms, providing a sort of quality badge to help them attract other partners and customers.

The second security requirement in the win-win template deals with *after* the loading process. The objective is to reduce significantly the risk of tampering in transit, ultimately with comprehensive monitoring for contraband and intrusion. Much better visibility and control is necessary to reduce the risk of tampering in transit. Four complementary visibility and control technologies have produced intense interest, research, experimentation, and levels of deployment:

1. Biometric systems for positive identification of personnel, including truck drivers.
 2. Mobile communications, such as satellite or cellular, with global positioning system-like location determination.
 3. Sensors, both improved nonintrusive inspection devices and on-board sensors. These include portable devices to detect weapons of mass destruction, explosives, human presence, and intrusion. Eventually these could be built inexpensively into containers.
 4. Electronic cargo seals.
- All of these technologies have the potential to improve efficiency as well as security.⁴

Inspection and Process Control

U.S. Customs currently applies a blend of techniques to select shipments for physical inspection. The vast majority of incoming shipments are prescreened by the Automated Targeting System (ATS), a risk management system that applies data mining techniques to advance shipment information and historical data about the shipper and similar shipments. The ATS searches for anomalies, such as surges in shipments or a single shift to a new source or route. Most candidates for advanced screening and physical inspection are chosen based on these results. Customs is working to improve the ATS by integrating intelligence information and improving its algorithms.

A major approach to improve ATS prescreening is the 24-

We need to think about supply chain security more in terms of prevention, process control, and design improvements.

hour rule. The rule relates to the third security requirement in the win-win template—making accurate, complete, and protected information about shipments available to those who need it in a timely manner. When the rule is fully implemented, penalties will be levied and containers may be barred from entry into the United States unless detailed contents information is provided electronically to Customs at least 24 hours before the container is loaded on the ship. The rule would provide a meaningful window for the ATS review as well as an opportunity to divert questionable containers for inspection before loading aboard ship. While the ocean carriers generally support the rule, many shippers and shippers' agents are worried it would restrict freedom of action, impose new costs, and result in disclosure of proprietary information.

The next layer of screening is nonintrusive inspection, usually performed near the ship as containers are off-loaded. The tools of choice are large gamma ray and x-ray machines that scan for anomalies in cargo density or container configuration. Some of these devices are already in use, and more are

being added. Most customs officials also carry handheld radiation detectors, and larger radiation and explosives detection sensors may be used as well. A variation is manual screening based on the experience, judgment, or intuition of customs officers. When anomalies turn up in screening, containers are physically inspected.

The United States also is working with other governments to increase the effectiveness and reduce the impact of inbound inspections. The Container Security Initiative is an example of this. It seeks to push inspections and screening upstream to originating ports—a practice in line with the general quality principle of source inspection. The CSI focuses on the 20 ports that originate the most containers bound for the United States—the so-called megaports. The United States hopes that the CSI will lead to a series of bilateral agreements permitting the exchange of customs officers and more screening of shipments at the outbound ports.

By shifting some of the screening and inspection burden to origin ports, the CSI would generate both security and business benefits. The security benefits are reduced risk of terrorist events, such as catastrophic explosions aboard vessels or in the receiving ports. The business benefits are reduced risk that a voyage would be interrupted because of concerns about a particular container and more predictable movement of cargoes inland from the receiving ports.

Yet, the CSI's benefits come with trade-offs. First, inspection congestion may be pushed upstream to originating ports that may have more difficulty coping with it. Ports such as Singapore and Hong Kong, for example, have high throughput rates and very limited real estate. Thus, they are more susceptible than U.S. ports to congestion problems from small increases in average container dwell times. Second, a series of bilateral agreements may hamper the third supply chain item

in the win-win template—harmonize and standardize security processes. Supply chains can be more efficient if the security regime has harmonized and standardized security processes. (For example, the productivity of a terminal operator or shipper in Hong Kong would decrease if shipments to North America, Europe, and Japan all required different security processes.) So, while the CSI is probably a major step toward progress, it creates the downstream challenge of integrating varied bilateral and nonmember processes.

Source inspection must be followed by process controls to reduce significantly the risk of container tampering during transit. Launched in October 2002, Smart and Secure Tradelanes (SST) is an industry initiative to deploy the latest automated tracking, detection, and security technologies for containers entering U.S. ports. The idea is to identify and isolate potential tampering of containers in transit. Effective process controls like these should enable the majority of SST or similar containers to receive “green-lane” treatment through U.S. Customs, avoiding final inspection delays.



Implications of Prevention at the Source

Shifting attention from inspections at receiving ports to prevention at the source also implies significant culture changes. Most supply chain managers can see the advantage of adopting a quality-oriented point of view about security. Customs agencies, however, may have a harder job shifting their historical emphasis on imports to a much heavier concentration on exports.

Prevention at the source will certainly improve security assurance but, unlike the quality movement in manufacturing, it will not eliminate the need for inspections altogether. Given the law enforcement tradition and increased national security role of border crossing officials, U.S. Customs and other agencies will continue some inspection programs. Customs Commissioner Robert Bonner, however, recognizes that inspection is costly and subject to errors. Bonner also realizes that extensive inspections slow down supply chains and degrade operational performance. As a result, he has directed Customs to work towards enhancing the effectiveness of inspections rather than increase the inspection rate. Source prevention and better prescreening will enable inspectors to focus on a small number of high risk and questionable shipments.

Finally, it is worth reiterating the value of improved visibility and control. These characteristics that cut across the win-win template are critical to improving supply chain efficiency and effectiveness as well as to enhancing security. Improved visibility and control are essential for developing successful process controls and strategies for responsive reactions.

Mitigation Strategies

So far, the discussion has focused on preventing supply chain security breaches. Yet strategies also are needed that will mitigate the effects of a security breach once it occurs. Potential breaches range from “out of bound” conditions on shipments, through major security alerts and tightened governmental security constraints, to disruptions following terrorist attacks. Companies must be able to respond effectively to this wide range of security breaches. Responsive reactions could be in the form of providing direct relief to those parts of the supply chain affected by the security breach or creating alternatives that would work around the disrupted parts. Notably, many sound supply chain practices also provide sound methods for responding to security problems.⁵

The sections below detail six strategies that companies can adopt to mitigate a security breach. Many of these strategies incorporate principles of the quality movement and the win-win template, such as visibility, control, and design improvements. They also include key supply chain management concepts like flexible sourcing, effective inventory management, and demand-based management.

Strategy 1: Comprehensive Tracking and Monitoring

An effective response strategy centers on the ability to detect a security breach as soon as it occurs. Any out-of-control

problems must be detected promptly, and the exact location and nature of the problem isolated. In the case of supply chain security, companies need cost-effective monitoring systems in place for shipped items, reusable packing assets, and transport conveyances. These systems need to have robust data management capabilities to handle the flood of data and parse potential Type I (labeling a conforming item as nonconforming) and Type II (missing a nonconforming item) errors. In addition, the tracking systems should be able to prioritize discrepancies and help manage the corrective actions.

At present, there is no system that can affordably monitor every shipment continuously from origin to destination. But

An effective response strategy centers on the ability to detect a security breach as soon as it occurs.

progress is being made as more and more new technology solutions appear in this space, which is sometimes referred to as supply chain event management or supply chain performance management. These technologies need to provide real-time visibility and monitoring capabilities that identify a potential breach. They also must be able to alert the right parties when problems occur, connect these decision makers together, and help them implement actions.

For the decision makers, the visibility and monitoring system must be able to provide concrete and precise information on the specific areas affected by the security breach as well as the extent of the problem. It is more useful to be able to pinpoint specific containers, for example, than to simply isolate a trade lane with a potential problem.

Strategy 2: Total Supply Network Visibility

Having information on the rest of the supply network can help a company mitigate the effects of a security breach. When a security breach develops in one part of the supply chain, companies can respond more effectively if they have a clear picture of the location and form (raw materials, sub-assemblies, work in process, in transit, or finished goods) of other inventories in the supply network as well as the capacities of their suppliers, manufacturers, transportation providers, and distribution networks. This information enables them to immediately reroute goods, revise production plans, redeploy production resources, and adjust capacities. Having a clear picture of the supply conditions and service plans also helps to reduce customer anxiety while allowing companies to devise appropriate responses.

Such information visibility requires at least two things: (1) event-driven data of supply chain operations, including security chain-of-custody information and (2) a tight integration of information systems across suppliers, manufacturers, logistics providers, and customers. Cisco's eHub, a private



exchange, meets these two requirements. It links multiple tiers of suppliers and instantly provides all players with a complete picture of the potential supply shortfalls, capacity crunches, or other disruptions. The eHub is also equipped with problem resolution paths so that problems, once identified, can be resolved quickly.

Strategy 3: Flexible Sourcing Strategies

Since the 1980s, many companies have followed the Japanese manufacturing principle of streamlining the supply base. Ford Motor Company, for example, trimmed its supply base by thousands of vendors. Other companies even adopted a sole sourcing strategy. Supplier consolidation and reduction was supposed to help companies build stronger, longer-term relationships with their suppliers and reduce the

Given the risks of terrorist events, the sole sourcing approach may have to be revisited.

overheads associated with managing multiple vendor relationships.

Given the risks of terrorist events, disrupted flows, and potentially troublesome security countermeasures, however, the sole sourcing approach may have to be revisited. With a single source of supply, the closure of trade lanes or a disruption at the supply source could disable your supply chain. Alternatively, companies should consider following one or more of the following flexible sourcing strategies:

- *Develop multiple supply sources for the same component or input material in a manner that will cost effectively enhance flexibility.* While having multiple supply sources can create the flexibility needed to address security problems, it often adds significant costs. Hewlett-Packard Company (HP) has developed a new procurement strategy that combines flexibility with cost efficiency.⁶ The strategy calls for a fixed supply contract for guaranteed quantities with one supply source that specializes in efficiency. This would enable this source to achieve the highest cost efficiency. Next, another supply source that specializes in flexibility is given a flexible contract with upper and lower volume limits. Such a contract costs more per unit, but the added value of flexibility is worth it. Finally, if demands come in over and beyond the supply sources' fixed plus flexible quantities, HP relies on spot markets to make up the difference.

- *Create a local supply source.* For a long time, U.S. apparel companies have used local suppliers to supplement their main, offshore suppliers. Companies use these smaller-scale U.S.- or Mexican-based manufacturers to add responsiveness to their supply chain. A local supply base, although slightly more expensive, can respond to changing market needs much faster than the main, offshore supply base. A

local supply source strategy also can address security breach problems. If a disruption causes the closure of trade lanes between the United States and overseas countries, the second "local" source can be used to provide the necessary backup. HP uses this "dual response" strategy to manufacture DeskJet printers. The company produces the majority of printers in Singapore because of that country's lower cost structure. At the same time, it has supplemental manufacturing in Vancouver for fast response to the North American market.

- *Create multiple supply sources with the appropriate manufacturing capacities to build the component when needed.* Instead of having multiple suppliers for the same component, a company would merely reserve manufacturing capacity in several suppliers' facilities. These capacities could be tapped to manufacture different components when needed. While this approach involves an investment, it will provide the needed flexibility when one supply source is disrupted. For example, if a security problem disrupts one manufacturing facility, capacity at another supplier could be quickly adjusted to produce the disrupted supplier's components. Li & Fung, the Hong Kong-based supply chain integration company for the apparel industry, utilizes this strategy. The company works with fabric and garment manufacturers to reserve capacities for customers like the Gap, Disney, and Gymboree—even before the precise SKU-level of orders are available.

- *Use a supplier with more than one manufacturing site to supply materials.* Electronics manufacturing service (EMS) companies, for example, are using their extensive network of manufacturing sites to provide their customers with greater flexibility. The network allows the EMS provider to shift production from one site to another to avoid disabled sites and trade lanes.

Strategy 4: Balanced Inventory Management

Just-in-time inventory gave rise to an era of lean manufacturing and continuous trimming of inventory fat. Yet, because security-related problems or other disruptive events can easily upset supply processes, lean inventories make companies vulnerable to sudden stockouts. The recent labor problems at the U.S. West Coast ports illustrated this situation. As cargo and vessels backed up, many manufacturing sites, such as the NUMMI factory in Fremont, Calif., had to shut down their production lines because component inventories were not being resupplied.

Exhibit 2 illustrates the significant impact of delivery unreliability. The amount of safety stock kept to maintain a service target is a function of both the average and the variance of the delivery lead time.⁷ From this simple numerical example consisting of two cases (one for stable demand and one for variable demand), it is clear that reducing lead-time variability can cut safety stock more than reducing the average of the lead time itself. Interestingly, when demand is



more stable, variability of lead time is more harmful. Delivery unreliability can therefore be very costly to a company.

Recognizing the risk of delivery unreliability, some companies have revisited the soundness of just-in-time inventory control principles. While it would be easy to simply put inventory back in the supply chain to provide added protection, the cost of doing so can be very harmful. We could easily lose the discipline of quality processes and slip back towards the inefficiencies that prevailed in the '70s and '80s, when excess inventory created quality problems, poor management, wasteful processes, excessive warehousing, and costly write-offs. It is important for companies not to over-react.

Instead, to find the "right" level of inventory, companies should apply scientific inventory methods to assess the trade-offs between the risks of stockouts and the costs of inventory. To do this, it is now necessary to capture the risk of security-related supply disruptions. Most traditional inventory systems, however, only deal with demand uncertainties. Some companies have responded by using longer supply lead times in their inventory systems to adjust for the risk of supply dis-

ruptures. This does not fully address the problem. As Exhibit 2 showed, the right amount of safety stock is not just a function of the average lead time but also its variance. Companies therefore need to use inventory systems that can capture the uncertainties of both demand and supply.

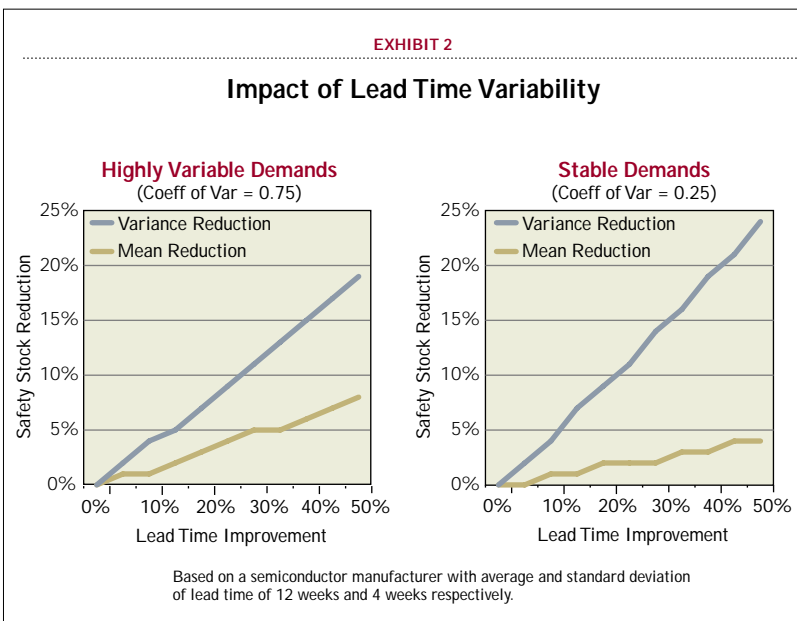
Strategy 5: Product and Process Redesign

“Design for supply chain management,” a management concept that emerged in the 1990s, means designing products and processes so that logistics, order fulfillment, and other back-end processes can be optimized.⁹ Out of this concept came the technique of “postponement,” or delayed product differentiation, which has been successfully applied in high tech industries such as computers, printers, and other telecommunications equipment sectors.

Companies can use such design principles to address the risks of security problems. Increasing component commonality, for example, enables companies to increase both the supply base for the component and inventory pooling with other sites. Standardizing the manufacturing process also allows companies to create more common production capacities so that capacities from different suppliers or locations can be utilized when disruptions occur. Postponement lets companies configure products at the last minute, which enables them to meet demands using alternative configurations if one component is in short supply because of security disruptions.

Lucent Technologies' 5ESS Switching System Group in Tres Cantos, Spain, utilized these design principles to successfully complete a major project for Saudi Arabia in the late 1990s. The project involved upgrading the country's telecommunications switching systems to be Y2K-compliant. Because the project was initiated in 1998, Lucent had less than two years to complete it before the Y2K deadline. This project created a huge demand surge for circuit packs and cabinets that the Tres Cantos factory was not able to handle. And because of process differences, Lucent could not use the capacities of its other factories in Oklahoma City, Poland, and Taiwan. By redesigning the product so that the bulk of it was standardized, Lucent was able to retool the processes at all of the other factories and ultimately use these facilities to complete the project on schedule. The redesign of the product and process enabled multiple capacities to be shared. Such capacity flexibility can help supply chains respond to both demand surges or supply disruptions.

In another example, when a lightning bolt caused a fire at its radio-frequency chip supplier's factory, Nokia quickly redesigned the chips so that they could be sourced from other locations. With the design change, Nokia was able to



Inventory management strategies are particularly effective when the information systems are integrated and give a comprehensive view of inventory location. This level of integration makes it possible to use a "networked" inventory approach. Under this approach, inventories at different locations can be pooled and used to support demands originating from different localities. Retailing has made extensive use of such inventory sharing mechanisms. Saturn has an integrated information system that provides daily information on the inventory positions of their retailers. This information enables the

meet its production target despite the fact that the fire disabled the original supplier's factory for more than a month.

Strategy 6: Demand-Based Management

The final strategy to help mitigate the effects of a security problem is demand-based management—or, offering the right products at the right prices so as to match supply with demand. When a security-related problem occurs, companies can use this sophisticated tool to induce customers to buy what is available and avoid items that are in short supply. Demand-based management requires a deep understanding of consumer preferences, including how they would respond to price changes and different product offerings.¹⁰

When day-to-day supply disruptions occur, companies that practice demand-based management often make dynamic changes to the product configurations that they offer. Dell Computer is one example. Because Dell uses the Web-channel in its direct sales model, it can make changes to its product configuration relatively easily. With that flexibility, the PC-maker can easily steer its customers to the product configurations that are in ample supply. Such a strategy is effectively supported by product designs that use both common and substitutable parts, postponement, and standardized interfaces.

No More Tears

We acknowledge that the added costs of security are far from trivial. But we are also convinced that it's possible to implement important security improvements in ways that enhance supply chain efficiency and effectiveness.

The quality movement in particular offers models that can be effectively applied to supply chain security concerns. Instead of final, end-product inspection, the quality movement emphasizes prevention, total quality management, source inspection, process control, and a continuous improvement cycle. These are all ingredients for successfully managing and mitigating the supply chain security risks.

We applaud the efforts underway to instill quality processes, to inspect products and containers at the points of origin, to use technology to automate the chain of custody, to monitor the process closely during transport, and to create transparency and visibility across the supply chain. Information, rather than physical inspection, is the preferred way to go.

In addition to these constructive efforts, we need to put in place a responsive system that can react promptly to security breaches and new restrictions. Such a system requires a well-prepared workforce, an infrastructure for information visibility and knowledge transfer, agile logistics systems and financial resources, and readiness for fast execution. That responsive system must also utilize innovative supply chain management concepts such as flexible sourcing strategies, design for supply chain management,

inventory pooling, and demand-based management. With such a system, coupled with initiatives already under way, it will be possible to enhance security while actually improving supply chain efficiency—or achieving supply chain security without tears.

Footnotes

- 1 *Quality Without Tears* by P.B. Crosby (McGraw Hill, 1984) was one of the best sellers on quality management. Its main theme is that companies can achieve high quality without incurring excessive costs and pains by putting in place proper management philosophies and approaches.
- 2 A good reference to total quality management can be found in http://www.qualityspecialists.com/iso/iso_9000/iso.htm.
- 3 "Freight Transportation Security and Productivity," U.S. DOT FHWA, April 2002, pp. ES vii-ix. (http://www.ops.fhwa.dot.gov/freight/transportation_security.htm).
- 4 Three sources are "Technology to Enhance Freight Transportation Security and Productivity," U.S. DOT FHWA, April 2002; "Electronic Cargo Seals: Context, Technology, and Marketplace," U.S. DOT Intelligent Transportation System Joint Program Office, July 2002; and "Automating Security: A Rationale For Electronic Cargo Seals," in prepublication draft. (http://www.ops.fhwa.dot.gov/freight/transportation_security.htm).
- 5 Another excellent reference for supply chain responses to security problems can be found in Y. Sheffi, "Supply Chain Management Under the Threat of International Terrorism," *International Journal of Logistics Management*, 12.2, 2001, 1-11. Also, see Joseph Martha and Sunil Subbakrahna, "Targeting a Just-in-Case Supply Chain for the Inevitable Next Disaster" *Supply Chain Management Review*, Sept./Oct. 2002.
- 6 Shah, J.B. "HP Wrestles Risk," *Electronics Buyers News*, Sept 24, 2002.
- 7 Standard inventory theory states that safety stock is a function of the square root of the sum of variance of lead time multiplied by the square of mean demand, and average lead time multiplied by variance of demand.
- 8 See M.A. Cohen, C. Cull, H.L. Lee, and D. Willen, "Saturn's Supply-Chain Innovation: High Value in After-Sales Service," *Sloan Management Review*, 41. 4, Summer, 2000, 93-101.
- 9 See E. Feitzinger and H.L. Lee, "Mass Customization at Hewlett-Packard: the Power of Postponement," *Harvard Business Review*, 75.1, 1997, 116-121, for more details of the postponement and design for supply chain concepts.
- 10 Examples of how companies can apply demand-based management concepts to create significant values can be found in H.L. Lee, "Intelligent Demand-Based Management," *International Commerce Review: ECR Journal*, 2.1, Spring, 2002, 61-73.

