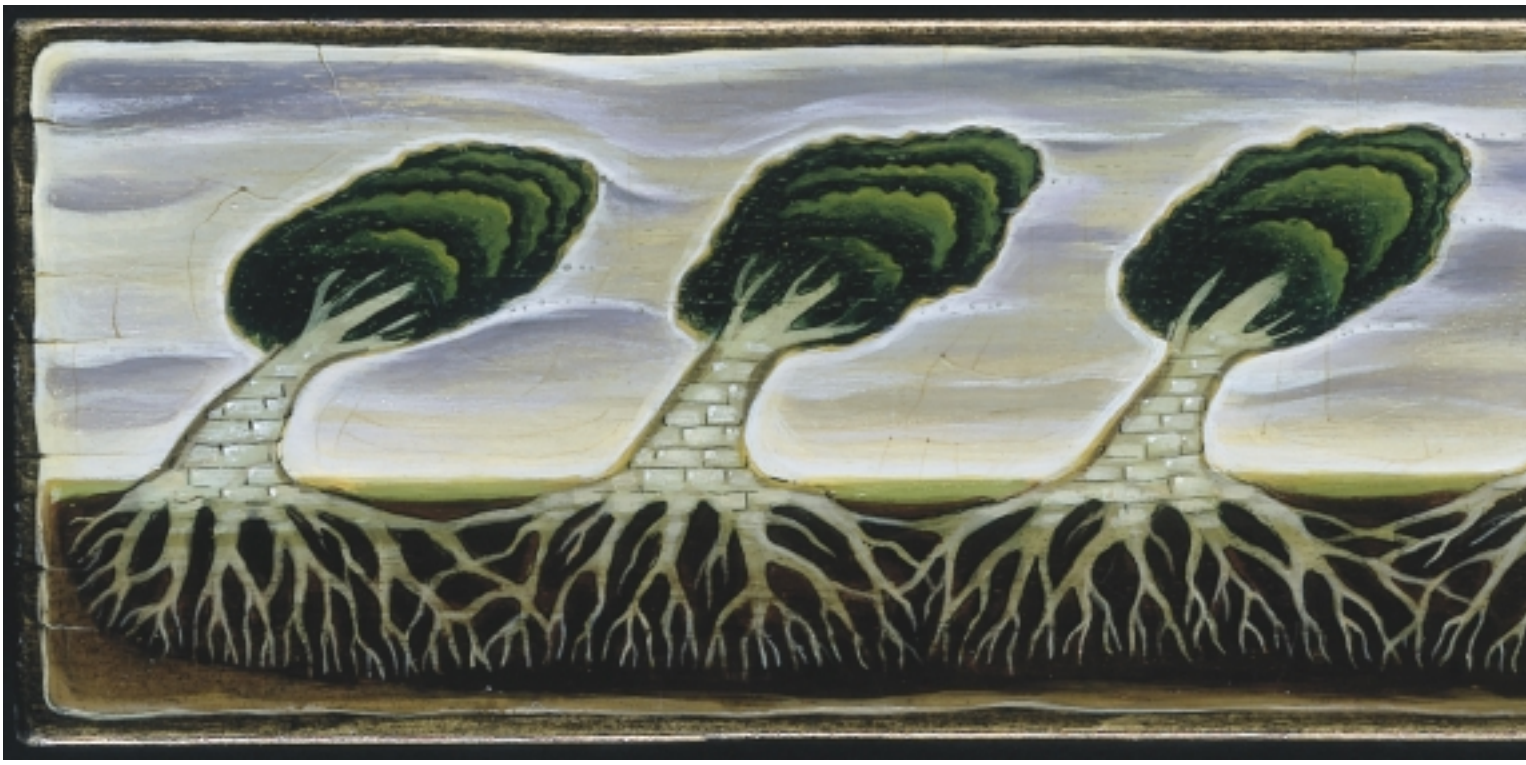
Building a SECURE AND

By James B. Rice, Jr. and Federico Caniato

James B. Rice, Jr. is director of the Integrated Supply Chain Management program at the Massachusetts Institute of Technology (MIT). Federico Caniato, a doctoral candidate at Politecnico di Milano in Italy, was recently a visiting student at MIT.

Are you gambling with your supply network? As we look back on supply chain management pre-Sept. 11, 2001, it's fair to say that many companies were indeed unwittingly gambling. Sadly, it took the terrorist attacks and subsequent reactions to expose a cold reality: The supply network is inherently vulnerable to disruption, and the failure of any one element in it could cause the whole network to fail. Further, the attacks dramatically illustrated the interdependence that exists in the supply network—not just among the trading partners but also with the U.S. government agencies involved in the flow of goods and the transportation infrastructure.

This new operating environment calls for a supply network design that is both secure and resilient. That means a supply network that has advanced security processes and procedures in place, while at the same time being resilient enough to respond to unexpected disruptions and



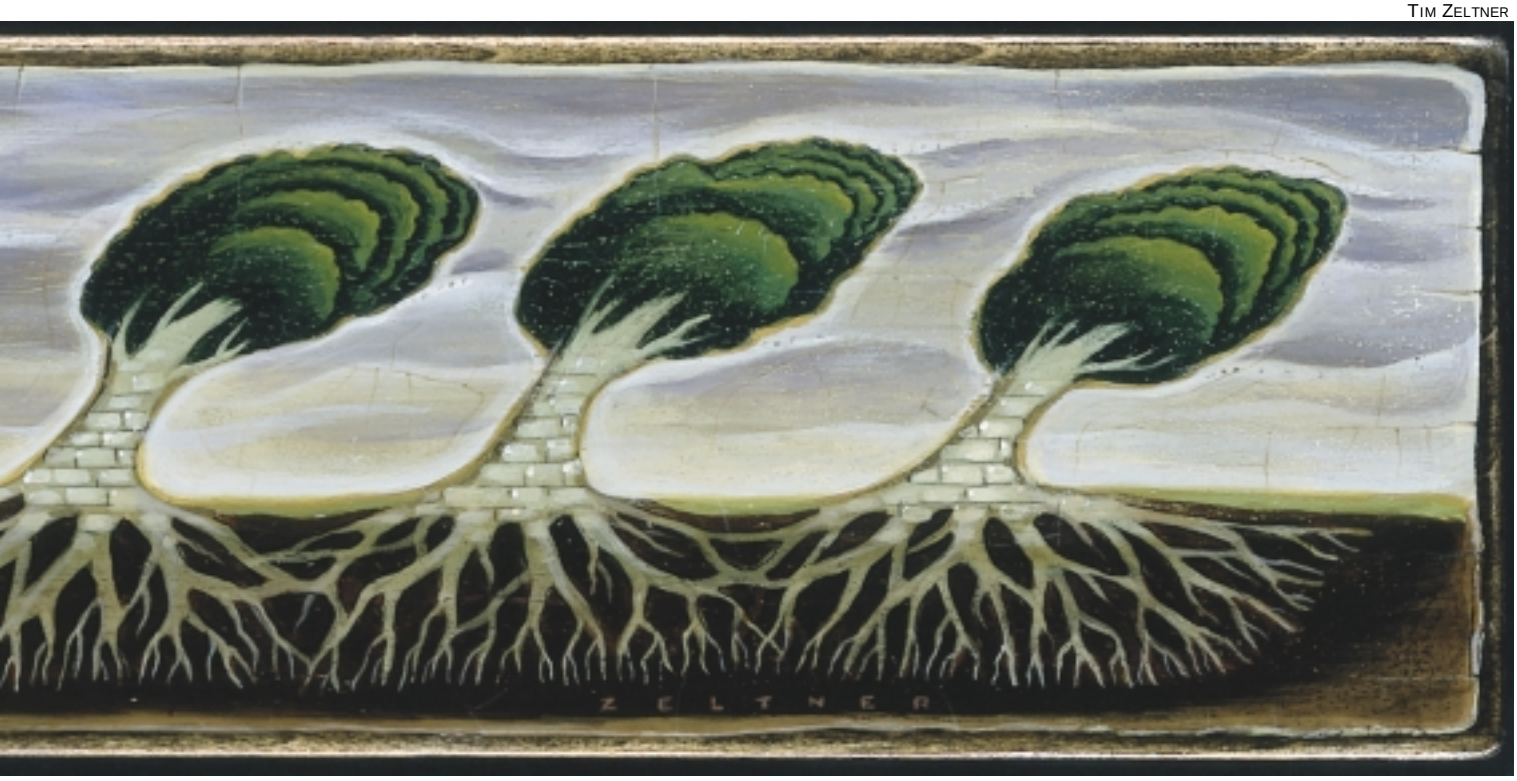
For many companies, the only thing standing between them and a disastrous supply chain disruption is luck. But, as any gambler knows, your luck eventually runs out. In today's business environment, you need a supply network that has comprehensive security processes and procedures in place and is resilient enough to bounce back from any disruptions that do happen. Luck plays no part in the equation.

RESILIENT Supply Network

restore normal supply network operations. Certain initiatives will provide the dual benefits of supply network security and resilience. Others will contribute to either security or resilience but not both. Ultimately, companies will need to design for both security and resilience, as a secure supply network does not guarantee a resilient supply network, and vice versa.

Today's operating environment also calls for new organizational capabilities. Specifically, companies will need to forge new relationships with those U.S. government agencies that now also are working to make supply networks secure and resilient. Similarly, deeper relationships need to be developed with suppliers and customers to co-create a more secure and

TIM ZELTNER



The "Response to Terrorism" Study

The "Supply Chain Response to Global Terrorism" project, conducted by the MIT Center for Transportation & Logistics, has examined the response to terrorist attacks from several different perspectives: the manufacturing and distribution industry response, the risk management and insurance industry response, and the U.S. government response. The project also studied how companies have responded to past disasters in the hopes of identifying useful analogies that could inform and enrich the Center's work.[1]

The organizations selected for the interviews were medium to large companies with operations in the United States and with supply chain subsidiaries or branches overseas. Semistructured interviews were conducted with a sample of 20 companies spanning a range of industries from high tech and aerospace to pharmaceuticals and consumer packaged goods. The sampling was based on an informal method that combined self-selection and convenience criteria—that is, those firms expressing an interest in the study and those with which the Center had an existing relationship.

Additional information on the research project study can be accessed at the project Web site, http://web.mit.edu/scresponse.

resilient network. Internally, the biggest organizational challenge may be to give individuals a solid understanding of the interdependencies and operational imperatives that now exist.

The Center for Transportation & Logistics at the Massachusetts Institute of Technology (MIT) initiated a research project to study how organizations are responding to this new environment. The study sample included major global companies from a wide range of industries. (For more on the project, see the sidebar "The 'Response to Terrorism' Study" above.) Overall, we observed a broad range of responses, the majority of which can be characterized as reactive—that is, the actions taken were in response to government regulations and other mandates. For those companies responding solely to mandates and regulations, the only thing that may be standing between them and a major supply chain disruption could be luck.

In a few notable cases, however, we observed companies executing against previously established plans and honing and refining their supply network for security and resilience. Notably, most of the companies in this advanced category had actually experienced supply chain disruptions in the past. What seems to set these leaders apart is their ability to learn from experience and take action to design and operate their supply networks to be resilient as well as secure. These organizations do not rely on luck but instead emphasize supply chain collaboration, intensive training and education, and sound strategy development. The sidebar "Classifying the Responses" on page 27 presents a summary of the corporate responses, classified into four levels of initiatives—from basic to advanced.

A first step in creating a supply network that is both secure and resilient is to recognize that the two are not the same. This distinction becomes important when developing plans focused on security and resilience respectively.

Yet while security and resilience are independent of one another, our study revealed that some types of responses address both—that is, they enhance security *and* resilience of the supply network. These responses center on such activities as business continuity planning, designing systems to "fail smartly," using layers to provide backups, aggressively training people in the organization, and making security and resilience a part of the company's culture.

The sections below describe those key actions that can improve security as well as those that can enhance resilience. Also described are the types of initiatives that address both, thereby bringing dual benefits.

Actions to Improve Security

Our study found that companies typically undertake a series of security initiatives to protect their supply chain from disruption. These responses can be classified into three groups: physical security, information security, and freight security. These groups, in turn, can be further segmented into two levels of response, basic and advanced. The basic level involves traditional activities that have become almost standard practice today. The advanced responses entail more forward-thinking initiatives, used by relatively few companies. The table below summarizes supply chain security measures at the two levels.

Supply Chain Security Measures

	Basic Responses	Advanced Responses
Physical security	■ Access control, badges. ■ Gates, guards, camera systems.	■ Extensive background checks. ■ Vulnerability testing by outside experts.
Information security	■ Hardware: firewalls, dedicated networks, etc. ■ Software: intrusion detection, anti-viruses, passwords, etc.	■ Audits of partners' information systems (IS) security. ■ Education and training for IS security.
Freight security	■ Inspections. ■ U.S. government initiatives (for example, C-TPAT, Container Security Initiative, Operation Safe Commerce). ■ Cargo seals.	■ Documented "standards of care," use of certified third parties, defined and vetted chain of custody. ■ Industry initiatives to establish standards of care among shippers and carriers. ■ Global positioning systems (GPS), radio-frequency identification (RFID), e-seals, biometrics, smartcards, sensors, etc.

We don't necessarily conclude that every company should adopt advanced responses. Those that have done so among our survey sample are organizations highly exposed to risk. Companies with less exposure could be sufficiently protected by the basic measures.

One aspect of supply-network security merits particular attention—employee screening and hiring practices. The leading companies have developed a core competency of preventing the "enemy from within" from being hired in the first place.

But even among the most security-conscious companies, effective screenings need to extend beyond the hiring process to include ongoing tracking and assessment of each employee and third-party provider with security access. This requires careful record keeping to alert the company to potential threats from anyone with enough knowledge and access intent on defeating the security system. While this may seem extreme, if such a procedure had been in place, it may have prevented a previously trusted third party from releasing nearly one million liters of raw sewage into local rivers from a wastewater plant in Australia. The offender was a contractor who installed the wastewater control system and who was subsequently turned down for a position at the wastewater plant. In retribution, he used his knowledge of the system to penetrate the plant and release the sewage.[2]

Ultimately, companies will need to design for both security and resilience, as a secure supply network does not guarantee a resilient supply network, and vice versa.

The hiring and screening process poses special challenges for transportation companies. With motor carriers, for example, the security of their operations can be dictated by the driver's activities and attitude. Yet background information on driver job applicants can be difficult to access. In some cases, records are kept at county levels within states, making it difficult and costly to identify drivers with poor track records in advance of hiring. A proposed federal Transportation Workers Identification Card (TWIC) may provide a common database for assessing a driver's security level, but this is a long way from implementation. In the meantime, companies need to be as vigilant as they can in conducting background checks during the hiring process.

Actions to Improve Resilience

Just as some initiatives focus squarely on security, others are directed toward resilience. In materials science, resilience is the physical property of a material that can return to its original shape or position after a deformation that does not exceed its elastic limit. In today's business environment, resilience is widely used to characterize an organization's ability to react to an unexpected disruption, such as one caused by a terrorist attack or a natural disaster, and restore normal operations.[3]

Beyond enabling a company to maintain operations following a disruption, resilience potentially can be a competitive advantage if you can respond more favorably to disruption than the competition. This might mean being ready to capitalize on opportunities to serve your competitors' customers if your competitors cannot.

Even in cases where the disruption affects the competitors equally, companies can compete on their resilience capabilities. This was evident in the respective responses of Nokia and Ericsson to the loss of a supply of radio-frequency chips (RFC) in early 2000. While both competitors depended solely on Philips Electronics for RFCs and were thus equally affected by a fire in the main Philips RFC plant, their responses could not have been more different. Nokia immediately sensed the disruption and responded aggressively, dedicating 30 employees to work with Philips and other suppliers to maintain a steady RFC supply. Ericsson, on the other hand, did not sense the seriousness of the disruption and ultimately mounted only a modest effort to restore supply. The net effect was that Nokia achieved its sales plans, while Ericsson missed a critical new product introduction that amounted to an estimated $400-million-revenue loss. Ericsson ultimately exited from the business of making cellular phones.[4]

Resilience through Flexibility and Redundancy

Of all the ways to create resilience, two methods hold the greatest potential. One involves flexibility, the other redundancy. Each approach has different cost and service characteristics that are important considerations when designing a supply network for resilience.

Flexibility entails creating *capabilities* within the organization to respond. These capabilities are mainly developed through investments in infrastructure and resources before they actually are needed. Initiatives to improve flexibility would include, for example, developing a multi-skilled workforce, designing production systems that can accommodate multiple products and real-time changes, and adopting sourcing strategies that permit transparent switching of suppliers. By using flexibility, the company redeploys some existing capacity in one area to make up for lost or delayed capacity in another area. This involves some costs for designing rapid change operations that accommodate multiple products and for developing a multi-skilled workforce.

Redundancy, by contrast, entails *maintaining capacity* to respond to disruptions in the supply network, largely through

investments in capital and capacity prior to the point of need. Redundancy is central to such efforts as managing inventory, maintaining production lines or facilities in excess of capacity requirements, committing to contracts for material supply (buying capacity whether it is used or not), and maintaining a dedicated transportation fleet.

An important distinction between flexibility and redundancy is that the latter involves capacity that may or may not be used; it is this *additional* capacity that would be used to replace the capacity loss caused by a disruption. Flexibility, on the other hand, entails redeploying previously committed capacity. This implicitly involves making tradeoffs among producing different products or serving different customers, which would not be the case with redundancy.

Ultimately, a company will likely adopt a mixture of these flexibility and redundancy alternatives, depending on different cost and service characteristics as well as on specific business and industry factors.

Additional Responses to Create Resilience

In addition to the approaches just described, respondents to our survey reported pursuing many other actions to enhance resiliency in their supply network. The range of these responses, not all of which are new, suggests that no single approach fits all situations. Exhibit 1 lists those responses, categorized by failure mode—that is, by disruption in supply, transportation, facilities, communications, or human resources. It's important to focus on the failure mode for this reason: While there are unlimited sources of disruption, there are relatively few failure modes. Addressing the failure mode, therefore, facilitates action and gets the organization moving toward an appropriate response.

For each response listed in the exhibit, we present the respective advantages and disadvantages. Ultimately, a company needs to pursue those particular responses that make the most sense for them based on a range of operational and market factors. There is no one single "silver bullet" response.

Note that many of the responses listed in the exhibit revolve around the decision to sole source or dual source for capacity.[5] Equally strong arguments exist for both approach-

EXHIBIT 1

Supply Chain Resilience Responses by Failure Mode

Resilience to Disruption in…	Action	Advantages	Disadvantages
Supply	Use multiple and/or local sources in different locales.	Spreads risk across two firms, two locations; local source protects against international supply shortages.	Higher cost to qualify supplier, lower volume leverage, no assurance additional supplier is more resilient.
	Use single source.	Known supplier, high supplier commitment, leveraged volume.	Vulnerable to disruption unless supplier has multiple flexible sites, backup plans.
	Contract for supplier flexibility.	Contract obligates supplier in advance.	Potentially higher cost per unit, may entail fixed costs for "take or pay" committed volume.[6]
	Modify inventory levels.	Right parts inventory and risk pooling may reduce inventory costs.	Requires periodic analysis by item as conditions change.
	Modify product to use standard parts.	Reduces part and inventory cost, complexity.	Costly to modify existing materials standards.
Transportation	Prepare for and use multiple modes and carriers.	Pre-disruption relationship ensures support in crisis.	May need to commit volume to the alternate modes to get access in a disruption.
	Use spot market for capacity.	Efficient transaction with no upfront or lasting commitment.	Unknown carrier means added risk, potential for exceptional high pricing.
	Use logistics providers to source transportation.	Providers may have greater leverage and access.	Requires commitment (volume, cost) and relationship with logistics provider.
Production Facilities	Use multiple sites, each making multiple products.	Enables shifting production around locations.	Requires standardization in production operations, additional capital for additional facilities.[7]
	Modify inventory levels and policies.	Right finished-goods-inventory levels and risk pooling may reduce inventory costs.	Requires periodic analysis, potential redesign of supply network.
	Modify product to use standard processes.	Leverages common processing capabilities for lower cost, easier backup available.	Costly to modify product and production processes.
	Identify and contract backup production facilities.	Committed backup assured, potential to co-locate at supplier or customer.	Not dependable without contingency contract for the facilities in disruption.[8]
Communications	Use range of communication media.[9]	Communication in nearly any event.	Must maintain broad range of old and new technology.
	Back up data.	Protects against data loss.	Still requires physical system in event of system loss.
	Contract for backup IT system.	Provides for near-term system availability.	Potential delay in immediate response to massive system disruption.
	Set up and operate parallel or mirrored IT system.	Affords immediate system availability.	Requires cost to build, operate, and maintain separate system in protected environment
Human Resources	Develop cross-trained workers.	Enables shifting of employees and production as needed.	Must cross-train employees, and modify work system to utilize multi-skilled employees.
	Modify production process for unskilled labor.	Allows rapid increase or decrease in capacity.	Requires simplification of production process (not always feasible).
	Back up knowledge.	Best practices captured and documented.	Requires significant investment to capture and maintain knowledge in useful form.

es. In the end, the company will need to trade off the risk mitigation and cost factors of multiple sources and locations vs. forging closer, more responsive sole-source relationships.

Activities to Achieve Security *and* Resilience

To this point, we've discussed actions to increase either the security or the resilience of the supply network. But beyond these actions, certain responses can provide dual benefit to security *and* resilience, although not necessarily in equal measure to both. These responses are more likely to gain wider support because they typically have more tangible benefits associated with them and thus have a broader appeal across the organization.

Business Continuity Planning

Broadly speaking, business continuity planning (BCP) means developing plans to be resilient—that is, to be prepared to respond to and restore operations after an unexpected, major disruption occurs. Focusing on BCP also improves security by virtue of exposing the potential weaknesses in the system, and then focusing efforts to address those weaknesses. Implicitly, business continuity planning also helps companies make better decisions with regard to how much resilience and security is desired, how to achieve the target levels and through what measures, how to develop backup plans, and so forth.

At the more progressive companies, BCP entails establishing multiple layers of security and resilience. Typical layered actions include early and ongoing assessment of supplier security and resilience through on-site visits and quarterly "capacity reports" (in-person assessments of the real-time capacity available at the time of inquiry); development and maintenance of alternative supply and production capacity; mirrored information systems with alternative communication system backup; and specific plans for an emergency response to disruption. The layered nature of the business continuity plans means that each response does not need to be perfectly implemented because the layers of security and

Classifying the Responses

Level 1—Basic Initiatives. Companies engage in fundamental security and preparedness activities.

- Physical security measures: Access control, badges, guards, camera systems.
- Personnel security: Criminal, credit, and background checks on potential employees.
- Standard risk assessment: Consideration of risks such as fire, flood, vandalism, and disruptions to utilities.
- Basic cyber security: Anti-virus software, firewalls, passwords.
- Continuity plan: Responses for small-scale incidents to recover internal operations.
- Freight protection: Employee background checks, cargo seals, tracking technologies, sensors.

Level 2—Reactive initiatives. Companies meet or exceed the Level 1 practices and show greater awareness of security vulnerabilities.

- Larger security, risk, or business continuity organizations: Heightened commitment through reallocation of human or capital resources.
- C-TPAT compliance: Application filed for compliance with Customs-Trade Partnership Against Terrorism.
- Analysis of supply base: Assessment of supplier response capabilities.
- Supply continuity plan: Development of dedicated continuity plans.
- Limited training: Select employees educated/trained on Level 1 and 2 initiatives.

Level 3—Proactive Initiatives. Companies meet or exceed Level 2 and adopt security and resilience practices beyond industry norms, government regulations, and supplier or customer requirements.

- Executive-level leadership: Position such as director or chief of security established.
- New skills added: People hired with prior military, law enforcement, or intelligence agency experience.
- Structured risk assessment: Formal and comprehensive approaches to analyze company's exposure to risk.
- Advanced cyber security: Intrusion detection systems in place, relocation of information systems in secure buildings, physical separation of the internal network from the Internet, auditing of partners' practices.
- Business continuity plan: Plans to address primary failure modes, often developed in collaboration with logistic providers.
- Industry and security participation: Participation in development of industrywide common policies, standards.

Level 4—Advanced initiatives. Companies in this group meet or exceed Level 3 and often lead progressive resilience and security initiatives. Only a few companies have reached this level.

- Customer-supplier collaboration: Flexible contracts, joint continuity plans developed with suppliers and customers.
- Learning from past disruptions: Past experiences used as guide to make their organization stronger.
- Formal security strategy: Comprehensive, documented strategy that includes all initiatives to increase supply chain security and resilience.
- Supply chain drills, simulations, and exercises: Training and exercises that include simulations of supply chain disruption and stress testing of security measures and business continuity plans.
- Emergency control center: A predetermined facility and set of procedures to manage and coordinate the response to unexpected disruptions.
- Cost/benefit quantifications: Actual or expected costs and benefits of different alternatives are quantified.

resilience actions back each other up. Hence a layered system could remain secure and resilient even though one of the layers may have been defeated.[10]

Some advanced companies have established emergency operating centers (EOCs) to facilitate their response plan. Set up in a protected working environment within the organization, these centers provide a venue where a predetermined set of leaders convene to make decisions about the business. Each EOC has all the communication devices necessary to reach key decision makers and business operators, thus providing a defined working environment, hierarchy, decision-making process, and operating procedures for responding to disruptions. Localized disruptions activate the local EOC. When the disruptions span beyond the scope of one facility's operations, a global EOC is activated.

Responding through Organizational Capabilities

One of the more powerful capacities observed from our study was the ability of certain companies to improve security and resilience through their organizational capabilities. Specifically, these leaders have been successful in "socializing" security and resilience—that is, making these qualities part of the organization's culture and accepted set of beliefs.

Before any proposed initiatives to improve security and resilience can move forward, the business case for such investments needs to be made.

This is accomplished largely through enterprise-wide training on security and resilience and incorporating these characteristics into the course of daily operations and decision making.

A recent conference held at MIT underscored the importance of socializing security in the organization.[11] Specifically, several attendees reported improving security and supply network performance by bringing together the organization's security and supply chain functions. One company accomplished this informally via a project team comprised of security and logistics leaders. The team was charged with executing a "sting" operation intended to catch an organized theft ring that had been hijacking freight en route. This multifunctional team succeeded where independent logistics and security efforts in the past had not. Another participating company put a formal, long-term structure behind the security-logistics connection by re-assigning five security team members to the global logistics team.

Security and resilience also can be enhanced by the organization's leadership. Almost all of our respondents, in fact, had elevated the top security position to chief security officer, director of security, or a similar title. Increasingly, these top managers are being tasked with responsibilities that incorporate aspects of both security and supply network operations.

Similarly, the skill sets of leading companies have expanded, largely through the hiring of outside experts with backgrounds in federal law enforcement agencies or in the U.S. military. In addition, some U.S.-based global companies have enlisted security experts from non-U.S. law enforcement agencies such as the Israeli Mossad, Irish Garda, British Intelligence, and the Hong Kong Police. In this way, organizations are integrating security expertise into their supply networks (although a lot more integration still needs to take place).

Perhaps the most frequently noted organizational actions involve education and training. Leading companies educate their people (and their suppliers and customers) about security, resilience, and supply network risks. In doing so, they raise awareness and reinforce the importance of secure and resilient systems.

They also train their organizations on how to execute the emergency response plans through in-house training, typically including emergency response or supply network "fire drills." These simulations and exercises explicitly test the emergency response plan as well as the organization's capability to execute the plan. Drills and tabletop simulations involve mock exercises for different kinds of disruption. These exercises assess the disruption's impact not only on individual facilities but also on the entire supply chain. This is done by company employees actually checking supply material availability at key suppliers, transportation providers, or other "disrupted" parts of the supply network. The most progressive companies periodically surprise local facilities and announce a "supply network disruption drill." This action activates the EOC for mock operations, which includes interaction with local authorities, customers, and suppliers.

Making the Business Case

Before any proposed initiatives to improve security and resilience can move forward, the business case for such investments needs to be made. And that case is made most forcefully when the impacts are quantified.

The difficulty, however, comes in trying to quantify the impact of a supply network disruption *not happening*. As one respondent to our survey said, the real benefit in such cases comes from avoiding losses. "Nobody gets credit for solving problems that did not happen," this individual noted. This reality challenges the business to value savings from avoidance—a challenge that other cost-avoidance efforts, such as lean production, total quality management, and customer service improvements, already have addressed in some measure.[12]

A select few companies, however, have been able to quantify the impact of potential disruptions. For example, one company we surveyed estimated a $50 million to $100 million cost impact for each day of disruption in its supply network. Several others measured disruption in terms of time-to-customer impact—that is, the number of hours before a disruption ultimately affects a customer. One respondent resorted to building a separate, redundant production facility when it determined that a specific disruption would cause a cash-flow problem that would make the company insolvent in 30 days.

How effectively a company can quantify the impact may also depend on its ability to identify the collateral benefits of various investments in security and resilience. An investment in radio-frequency identification (RFID), for example, can improve not only security by tracking and monitoring cargo movements but also shipment visibility. And better visibility can translate to lower inventory requirements and improved service levels. Shippers and carriers that are developing "standards of care" for how to handle and protect shipments certainly will benefit from avoiding freight loss and damage. But they also will benefit from the resulting reduction in claims administration and lower insurance premiums. Investments in training on supply network risk and awareness have already produced a significant benefit for the city of Toronto. One may argue that officials in Toronto responded to the SARS (severe acute respiratory syndrome) outbreak early largely because they were alert for bioterrorism attacks—even though the outbreak was not an act of bioterrorism

Feeling Lucky?

Managers have a wealth of options available for designing a supply network that is both secure and resilient. But any effort will likely fall short unless an adequate business case is made for investing in network security and resilience. And the business case cannot be made successfully unless the impact of a disruption is quantified to some degree. Critical to making the business case and quantifying the impact is recognizing that the company is dependent on external entities for network security and resilience—and not just on internal business operations.

A key lesson from our study, in fact, centers on the weakness of focusing solely on internal operations by considering only the likelihood of a terrorist attack or major disruption on your company. Because the probability of such an event is very low, some may feel lucky and not work to make their supply network secure and resilient. But the more prudent perspective is to recognize that your supply chain may be disrupted by events or sources that are completely external to your organization.

Ultimately, what determines whether or not a company takes action may actually come down to its organizational capabilities to learn and be motivated from past experiences, rather than the availability of new technologies or risk assessment methodologies. In all but one case, the survey respondents with the most progressive security and resilience initiatives had already suffered significant loss from a previous disruption.[13] Each of these companies has since developed business continuity plans and more secure and resilient operations. So companies ought to ask themselves whether they prefer to plan for disruption and build the requisite organizational capabilities or to ask themselves every day, "Do I feel lucky?"

Authors' Note: The authors wish to recognize the significant contributions and project leadership by Yossi Sheffi as well as the individual contributions of the following members of the MIT research team: Jonathan Fleck, Deena Disraelly, Don Lowtan, Chris Pickett, and Reshma Lensing.

Footnotes

[1]Additionally, the project is developing the use of real options to assess the potential value of flexibility in supply chain design in responding to disruption. This research is being conducted by Richard de Neufville of MIT. For additional information, refer to http://ardent.mit.edu/real_options.

[2]See Reshma Lensing "Historical Events and Supply Chain Disruption: Chemical, Biological, Radiological and Cyber Events" MIT MLog thesis, June 2003, p. 46.

[3]Coutu, D.L. "How Resilience Works," *Harvard Business Review*, May 2002.

[4]Mukherjee, Amit. *Planning for an Ambiguous World*, Forrester Research and CommerceNet, March 2003.

[5]The trade-off between sole and dual sourcing has been noted in previous work, including Y. Sheffi, "Supply Chain Under the Threat of Terrorism," *The International Journal of Logistics Management*, vol. 12, no. 2 (2001), pp. 1-11.

[6]Byrnes, J. and R. Shapiro. "Intercompany Operating Ties," Harvard Business School Working Paper 92-058, 1991.

[7]For example, Intel's Copy Exact policy ensures all semiconductor fabrication plants are exact replicas.

[8]One automotive supplier succeeded in restarting operations in two days after a fire destroyed a factory by utilizing local facilities that had similar production capacity.

[9]One firm maintains ham radios to provide communication between all facilities in case of a complete information system disruption.

[10]Committee on Science and Technology for Countering Terrorism. *Making the Nation Safer*, National Academies Press, 2002, p. 214.

[11]Freight Lane Security in the Supply Chain Conference, sponsored by the MIT Center for Transportation and Logistics, April 29, 2003.

[12]Sterman, J. and N. Repenning, "Nobody Ever Gets Credit for Fixing Problems that Never Happened," MIT Research Paper, July 2001.

[13]The exception was a firm that was compelled by an external corporate security audit that noted weakness in the network and required progressive action.