

THE Avascent REVIEW

No. 12

SEPTEMBER 2006

SUPPLY CHAIN MANAGEMENT

Mapping and Assessing Security Threats Across the Supply Chain

PRIVATE ASSET PROTECTION

A Performance-Based Model for Assessing and Addressing Security Risks

These articles were originally published in the Fall 2006 issue of *DFI Quarterly*, the predecessor publication to *THE Avascent REVIEW*



THE Avascent GROUP
analysis • vision • results

SUPPLY CHAIN MANAGEMENT

Mapping and Assessing Security Threats Across the Supply Chain

BY JAMES W. TINSLEY AND CHRISTINA V. BALIS

Supply chains are the backbone of all economic activity. They are conceptualizations of the flow of raw materials through the various processing, production, and delivery functions that ultimately supply products and services to end customers.

Businesses rely on them to receive and deliver goods and services. In the global marketplace, supply chains constitute valuable commercial assets and competitive differentiators. Governments also rely on supply chains as part of their daily course of business but have an additional interest in protecting critical supply chains with homeland and national security implications.

Supply chains are highly vulnerable to infrastructure failures, and global interdependencies make these vulnerabilities even more pronounced. The overlap of public and private assets and responsibilities further complicates risk management within the supply chain, often impeding effective coordinated action and the implementation of appropriate solutions.

This article outlines a framework for understanding supply chain security with particular emphasis on

the intersection of public and private infrastructure and assets. It identifies common causes of supply chain security failure and their spiraling consequences as a result of infrastructure interdependencies. The article enumerates some of the typical consequences of supply chain security failures and presents a vision for an integrated approach that relies on close cooperation between public and private stakeholders on the one hand and security providers on the other.

Supply Chain Security: A Framework

A supply chain can best be understood as a series of nodes and connectors that extend across the value chain of every product and service (see figure 1). A node can function as the final destination of a product or service or as an intermediary point between original source and destination (e.g., a first-tier supplier that relies on other suppliers for parts and material or a prime-tier government contractor that depends on a various subcontractors). The more complex the process, the lengthier the supply chain and the more nodes needed to deliver the product to its final destination.



James Tinsley is a senior associate at The Avascent Group

The transition from one node to another is facilitated (or sometimes impeded) by connectors. Connectors often form part of larger infrastructure networks, such as transportation or communications, but they also involve non-physical aspects such as regulations.

At any point along the supply chain, operations may be affected by any number of external disruptions, ranging from the loss of a supplier to a natural disaster to a terrorist act. Globalization of business further complicates supply chain security and private asset protection. Multinational corporations operate globally, while other corporations

chain security requires protective measures in two main areas: private assets and critical infrastructure.

Private Asset Protection

Private asset protection (PAP) covers all assets belonging to a company, to include people, facilities, information systems, and intellectual property. Companies with global reach and global interdependencies face additional challenges in protecting vital assets.

Physically securing facilities that are located outside the domestic area of operation is challenging, especially in areas of the world prone to conflict or still developing economically and socially. For example, a decision to open and operate an overseas facility must take into consideration the costs of securing such assets in the event of a major disruption. Additionally, international laws may rule out some measures of protection that are used domestically, such as surveillance, while other measures, such as personnel screening, may be more difficult when foreign nationals are involved.

The sudden war in Lebanon highlights the importance of taking these issues into consideration. Many areas of Beirut were benefiting from foreign investment. Foreign firms operating in the Lebanese capital were adversely affected by evacuations and physical damage. Closure or destruction of ports, roads, bridges and airports immediately cut off supply routes and brought supply chains to a halt.

Another risk associated with business operations overseas and the use of global suppliers is the potential for physical and intellectual property seizure or theft. A recent example of the risks that companies face when operating internationally occurred in April 2006, when Venezuelan President Hugo Chavez seized the oil fields of two foreign oil compa-



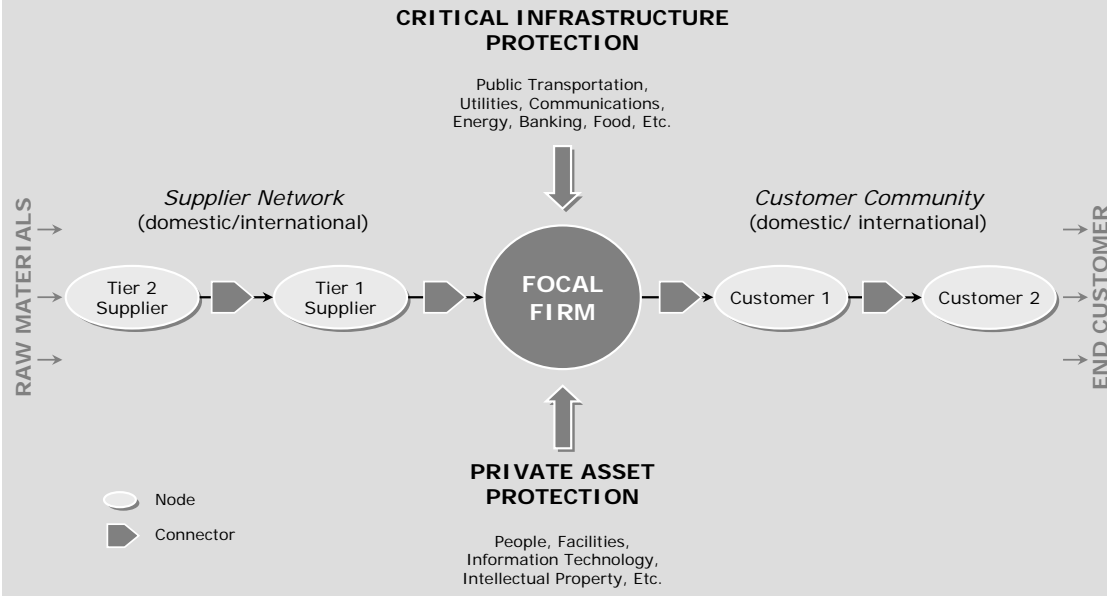
Christina Balis is a senior associate at The Avascent Group

receive raw materials and supplies from overseas vendors. Increased reliance on foreign supplies and global distribution networks necessitates that appropriate security measures and continuity of operations plans be in place to address various contingencies across the supply chain. Geopolitical volatility means that at any moment a supply chain could be interrupted or that operations could be disrupted. Detailed security assessments thus become increasingly important in understanding the risks associated with a dispersed supply chain.

From the point of view of any single node, supply

FIGURE 1

Integrated Supply Chain Security Model



shipping. Additional “key assets” identified in the report include national monuments and icons, nuclear power plants, dams, government facilities, and commercial key assets.³

Nearly all of these sectors and assets involve some degree of private ownership or operation. In fact, private companies

panies that had defied his plan to convert their existing operating contracts into joint ventures with PDVSA, the state-run oil conglomerate.¹

Critical Infrastructure Protection

PAP is closely intertwined with critical infrastructure protection (CIP). Critical infrastructure refers to “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”²

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, submitted by President George W. Bush in 2003, outlines 11 sectors of critical infrastructure: agriculture and food; water; public health; emergency services; defense industrial bases; telecommunications; energy; transportation; banking and finance; chemical industry and hazardous materials; and postal services and

own and operate 85 percent of our nation’s critical infrastructure and are responsible for protecting their facilities and restoring operations following an incident.⁴

What distinguishes PAP from CIP is not necessarily the type or nature of the asset but rather the level of public or private responsibility required for its protection—the same plant considered a private asset (say, a power plant belonging to a private utilities company) may also form part of critical infrastructure. Unlike PAP, which relies entirely on private sector funds and initiative, CIP is a shared responsibility between government and the private sector.⁵ As the administration’s recent review of the federal response to Hurricane Katrina points out, “Response planning must also recognize the unique Federal responsibility to support private sector efforts and assist in the restoration of critical infrastructures imperative to the National economy or integral to larger cascading systems or supply chains.”⁶

Supply Chain Interdependencies and Failures

The interdependence fostered between publicly and privately owned and operated infrastructure can lead to unforeseen consequences for both private and public supply chains. All supply chains are increasingly dependent on sophisticated infrastructure networks including transportation, power, and communications. It is these interdependencies that are increasing the number of potential targets and facilities at risk, the potential attack modes available to an intruder, and the overall consequences of attacks and natural disasters.

Broadly speaking, there are five categories of infrastructure, and consequently supply chain, interdependencies:⁷

1. **Input.** Material delivered by one type of infrastructure is used by another (e.g., telecommunications infrastructure generally depends on electrical infrastructure)
2. **Mutual.** Multiple infrastructure types serve as inputs for each other (e.g., oil pipelines and

- power generation are mutually dependent)
3. **Co-location.** Different infrastructure types located in the same geographic area (e.g., a power plant and a natural gas control center may be located in the same building, a dependency that can expand to a very large geographic area when infrastructure is threatened by natural disasters)
4. **Shared.** Infrastructure types that share physical components, transport, or facilities (e.g., telecommunications and power facilities share utility poles; infrastructure repair crews and fuel distribution rely on road networks)
5. **Exclusive.** Networks that can only support one or few outputs (e.g., oil pipelines cannot carry road traffic)

Infrastructure networks are generally resilient and have built-in redundancy to prevent mass disruption by a single or even multiple failures of any one component. However, infrastructure is vulnerable when multiple component failures have compounding systemic effects. Infrastructure system failures are therefore typically

grouped into three types: cascading; escalating; and common cause failures (see table 1).⁸

A cascading failure involves failure of high-volume nodes in a network that can spread quickly from one network to another through input and mutual interdependencies. An example would be electrical grids which, if attacked, can lead to cascad-

TABLE 1

Infrastructure Failures

FAILURE TYPE	INTERDEPENDENCIES	DESCRIPTION	TYPICAL CONSEQUENCE
Cascading	Input and Mutual	Disruption of high-volume nodes overloads the rest of the system	Network can collapse through damage to one node and without damage to any other node
Escalating	Shared and Exclusive	Disruption of one network prevents other networks from taking steps to compensate	Network cannot be repaired or restore itself
Common Cause	Co-location	Disruption of one physical site disrupts two or more networks simultaneously	Network is more thoroughly disrupted and redundancy is lost

ing failures as other downstream nodes shut down to avoid overload.⁹

In the case of an escalating failure, failure in one networked infrastructure can exacerbate failure in another due to shared and exclusive interdependencies. For instance, an attack against transportation, communications, or other networks would slow repair of an electricity failure.

Finally, a common cause failure stems directly from a single attack or disaster that has an impact on two or more networks simultaneously, usually due to geographical co-location. An example of a common cause failure might be an attack on a pipeline node that also destroys an on-site telecommunications node.

Even if an organization and its personnel are not directly threatened by infrastructure failure, its operations and supply chain can be severely disrupted. Such a disruption may affect critical parts suppliers, storage and distribution centers, as well as whole platforms. The impact of the disruption can extend all the way up to the end customers.

Infrastructure failure may be a measure of success for some terrorist groups. The obstacles to providing effective response in the immediate aftermath of 9/11 and Hurricane Katrina caused by damage to basic communication and transportation networks is not lost on potential foes. The casualties caused by disruption of response can be just as high as those caused by the incident itself.

The vulnerabilities of supply chains to cascading failure are exacerbated by business interdependencies. In one example cited in a study on the UK aerospace industry, the supply chain for a new system seemed secure until all of the competing subcontractors realized they were dependent on the same third-party supplier for a critical subassembly. As the

single source for the component, this supplier was overwhelmed with orders, and the overall schedule of the program was disrupted.¹⁰ If this basic supply chain limitation had been subject to further infrastructure or private asset disruption, delays could have escalated to the complete failure of the supply chain to deliver the new system to the government customer.

Consequences of Supply Chain Insecurity

Supply chain security attempts to mitigate supply chain disruptions—financial delays, operational paralysis, and even outright business collapse—that can arise from any number of man-made and natural hazards. The consequences of failed or inadequate supply chain security can take a number of forms, and all inevitably have an adverse impact on a company's bottom line. Governments face similar financial risks from failure to adequately secure their supply chains.

First-level financial costs from supply chain insecurity include product obsolescence, canceled or marked-down orders, penalties for non-delivery, and storage and transportation costs for excessive or mismatched inventory. These costs are certainly familiar to companies with long upstream and downstream supply chains. However, cascading effects from any number of supply chain security threats could affect a company's bottom line more severely than a typical disruption.

Overreactions to uncertain or distorted information, common in both man-made and natural incidents, can lead to chaotic consequences, which include mistrust of supply chain partners, second-guessing of previous sourcing decisions, and unnecessary intervention (as perceived by these other part-

ners) to mitigate risk. This not only exacerbates general inefficiencies in the supply chain, hence causing second-level financial costs, but can lead to a paralyzing “bullwhip effect” up and down the supply chain. An overreaction by an end customer, for instance, leading to a cancellation of long-lead orders can be disruptive for nearly every supplier.

Indirectly, a security threat to infrastructure can also cause massive disruptions. The US government’s decision to ground all flights and close US airspace for days following 9/11 due to lack of information on the scope of the attack and potential for additional hijackings was a paralyzing factor in many supply chains and an example of the bullwhip effect.

Finally, third-level financial costs from supply chain insecurity derive from market penalties due to a company’s inability to:

- Assemble a competitive bid package with demonstrated supply chain management past performance;
- Complete product development on time;
- Meet performance and product specifications;
- Adapt to changing market trends; and/or
- Capture short-lead customer orders.

While not exclusively reliant on security measures, market costs are ultimately the most important measure of performance when taking any steps to mitigate supply chain security risks. Ultimately, any supply chain security measures should increase confidence in both upstream suppliers and downstream customers that adequate efforts are made to mitigate all forms of risk. This transforms potential financial risks into a competitive advantage in the market.

Conclusion

Although steps have been taken to secure critical infrastructure throughout the United States, vulner-

abilities still exist based on the inherent design requirements of infrastructure networks. The overlap between private and public responsibilities inevitably leads to some conflicts over funding, which tend to slow preparedness efforts.


Supply chains are even more vulnerable than infrastructure networks, as many of their nodes and connectors are located at the intersection of public and private infrastructure and assets, public and private decision-making, and overall economic and social factors that are difficult to predict and nearly impossible to control.

Notwithstanding these difficulties, much can, and should, be done to secure supply chains. Governments need to secure infrastructure through CIP measures and mitigate the aftereffects of disruptions through strong emergency prevention, planning, response, and recovery efforts. Private companies need to take steps to secure both their property through PAP measures (including the development of strong continuity of operations plans) and their overall supply chains by analyzing them for points of failure and preparing contingency plans.

Security providers likewise face a number of new threats to their traditional business models. The vast array of threats and risks businesses deal with, coupled with the increasing complexity of business operations, calls for integrated security solutions that allow for full-spectrum planning, prevention, and response. No longer focused solely on facility security, private companies and government agencies want providers to assess vulnerabilities comprehensively and develop solutions for managing fully all supply chain risks—man-made, natural, accidental—that can disrupt or paralyze their operations.

It is beyond the scope of this article to go into all the steps that can be taken to secure supply chains.

Needless to say, many of these activities are based on analyzing supply chains more thoroughly and taking steps to build as much redundancy of suppliers and infrastructure as economically feasible. Moreover, converting this security investment into a marketing differentiator should be a key goal for passing whatever costs are accrued initially back to end customers. This process relies on strong customer and competitor analyses, as well as careful operational and organizational planning when implementing security plans.

Supply chains, and the infrastructure they rely on, will never be completely secure. However, with appropriate integrated security approaches, public and private stakeholders can mitigate the consequences of any failure in their supply chains and prevent worst-case scenarios. 

¹ Jens Gould, "Venezuela Tightens Oil Grip," *Christian Science Monitor*, April 14, 2006.

² White House, *The Federal Response to Hurricane Katrina: Lessons*

Learned, Washington, DC, February 23, 2006, p. 206, fn 72.

³ The White House, *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, February 2003, www.whitehouse.gov/pcipb/physical.html (September 10, 2006).

⁴ *Federal Response to Hurricane Katrina*, p. 81.

⁵ President's Commission on Critical Infrastructure Protection (PCCIP), *Critical Foundations: Protecting America's Infrastructures*, October 1997.

⁶ *Federal Response to Hurricane Katrina*, p. 206.

⁷ The discussion on infrastructure interdependencies and supply chain security failures draws on John Robb, "Infrastructure Meltdowns," Global Guerrillas Weblog, June 2, 2004, http://globalguerrillas.typepad.com/globalguerrillas/2004/06/infrastructure_.html (September 10, 2006).

⁸ Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine* 26, No. 6 (December 2001): 11–25.

⁹ For more detail on the modeled cascading effects based on attacks on complex network infrastructure nodes, see Adison E. Motter and Ying-Cheng Lai, "Cascade-Based Attacks on Complex Networks," *Physical Review E* 66, No. 6 (December 2002); http://chaos1.la.asu.edu/~yclai/papers/PRE_02_ML_3.pdf (September 10, 2006).

¹⁰ Marc Haywood and Helen Peck, "Improving the Management of Supply Chain Vulnerability in UK Aerospace Manufacturing," Proceedings of the 1st EUROMA/POMs Conference, Lake Como, Italy, June 16–18, 2003, www.som.cranfield.ac.uk/som/research/centres/lscm/riskpub.asp (September 10, 2006).

The Avascent Group

1717 Pennsylvania Avenue, NW
Suite 1300
Washington, DC 20006-4614

Phone: 202.452.6990

Fax: 202.452.6910

www.avascent.com

For more information on this
publication, please contact:

Christina Balis

cbalis@avascent.com

For more information on The
Avascent Group, please contact:

Jay Korman

jkorman@avascent.com

This is a publication of The
Avascent Group © 2007

The Avascent Group provides management consulting services to global leaders operating at the intersection of technology, business and public policy. Working with senior level management, The Avascent Group assists clients to become more competitive by making better, more informed strategic and tactical decisions on issues of strategy, marketing, operations and innovation in pursuit of their near- and long-term business objectives.

We offer our clients insightful analyses of today's changing business climate and how it affects their strategic outlook and market position. The Avascent Group specializes in:

Strategy Development

Market and Competitive Analysis

Industrial and Government Marketing
& Business Development Support

Merger, Acquisition, and Strategic Alliance Support

By combining our analytic talents with a deep understanding of the industries we serve and the broader political and policy context, we have earned a reputation for offering business leaders actionable recommendations and solutions to the challenges they face. We are set apart by our dedication to quality, timeliness, and pragmatism.

The Avascent Group's clients include leading and emerging companies in defense, aerospace, biotechnology, logistics, homeland security, and information technology.