

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-



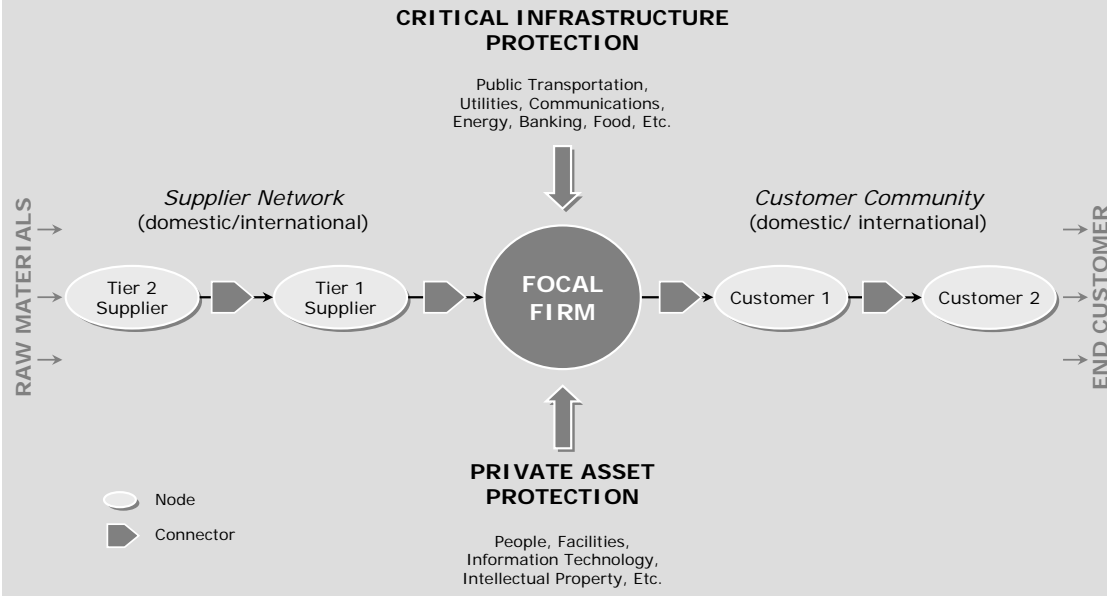
Christina Balis is a senior associate at The Avascent Group

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).

PRIVATE ASSET PROTECTION

A Performance-Based Model for Assessing and Addressing Security Risks

BY JAMES W. TINSLEY AND JACLYN LINDIG

Assets are at the core of every business transaction. Companies around the world rely on a wide range of assets—facilities, capital equipment, people, information technology (IT), intellectual property (IP)—to produce goods, provide services, manage deals, and function as independent commercial entities. When viewed from the perspective of the overall supply chain, private assets form a web of interlocking properties and people that depend on each other—as material suppliers, value-added manufacturers, and infrastructure operators—to deliver products and services to the end customer.

Private asset protection (PAP) in the United States was managed traditionally through a combination of private and public security, focused on loss-control measures and post-incident law enforcement respectively. These measures were never meant to provide total security. They were intended to cost effectively manage high-probability incidents, such as theft, fire and accidental destruction, while preserving a high degree of confidence in the supply chain. They were aimed at keeping businesses operating normally through a combination of deterrence and law enforcement.

The events of September 11, 2001 significantly

changed PAP requirements by highlighting the magnitude of the direct threat to private assets and the importance of PAP to overall critical infrastructure protection (CIP) schemes. The destruction of the World Trade Center and the consequent loss in corporate assets signaled a change in private-sector threat perceptions. Businesses now have to plan for low-probability, high-consequence events that challenge the traditional calculus of cost-effective security investment.

Security assessments conducted after 9/11 have emphasized the interconnectedness of private assets and public critical infrastructure.¹ As a result, subsequent public security initiatives have had increasingly to integrate PAP into their preparedness plans. Private companies, on the other hand, recognize their responsibility for implementing needed security enhancements. Although the government has not mandated security measures to date—instead recommending procedures and technologies based on CIP experience—private companies should do their best to head off potential government regulation through voluntary implementation of appropriate security measures.

This new emphasis on securing private assets and



James Tinsley is a senior associate at The Avascent Group

infrastructure creates opportunities and incentives for companies providing security services to redefine their offerings to be more relevant to the PAP market. Even new players without previous PAP experience may be able to leverage public CIP or systems integration experience to enter the market with a strong offering.



Jaclyn Lindig is a consultant at The Avascent Group

The Evolving Threat Environment

Before 9/11, PAP requirements focused on a defined set of traditional threats: man-made, both intentional (theft, vandalism, extortion, violence) and unintentional (workplace accidents), and natural

(earthquakes, hurricanes, tornados). These threats could be dealt with within a risk management framework that measured losses statistically and mitigated them through a combination of safety and security measures, insurance, and coordination with public authorities, including law enforcement, emergency management, occupational health and safety, and fire service agencies.

In this framework, the cost effectiveness of security measures was measured by the successful protection of irreplaceable assets (especially IP) and the implementation of procedures to maintain adequate insurance coverage at moderate premiums. In many

cases, safety measures were considered more important than security because of the prevalence of workplace accidents and the potential financial consequences of negligence law suits. When security measures failed, private firms would engage public law enforcement officials and take steps to ensure compliance with procedures on the books, again, primarily to ward off negligence liabilities. This mindset encouraged complacency among businesses.

The mass casualties and financial losses resulting from the 9/11 attacks forced private companies to reconsider their traditional security definitions and metrics. Three considerations, in particular, have driven changes in PAP security across the private sector.

First, companies now realize their exposure to terrorism risks. Previously, terrorism seemed to affect only limited segments of US industry, such as aviation. While there have long been terrorist bombings of nightclubs, restaurants and supply chain assets overseas, attacks on similar assets in the US had been rare prior to 9/11. Today, even the most benign private assets, such as shopping malls and theme parks, are potential targets.

Second, modern terrorists are more sophisticated than traditional criminal threats and more difficult to mitigate through traditional security measures. Terrorist training has increased significantly in technical and tactical effectiveness. No longer confined to weapons instruction and basic combat tactics, the modern training program teaches surveillance and counter-surveillance techniques and technologies, security testing and response procedures, improvised weapon construction and deployment, operational security, and full indoctrination.² Facing this level of threat sophistication, private companies cannot rely on the government to prevent all attacks and must

assume direct responsibility for intelligence and counter-surveillance operations.

Third, people who engage in traditional criminal acts, such as theft and violence, along with those participating in less harmful, yet potentially disruptive activities, such as protesters, are learning lessons and borrowing techniques from terrorists. The World Wide Web has expanded dramatically the availability of information on terrorist tactics, allowing criminals to become increasingly sophisticated with regard to target surveillance and operational security. The diffusion of these techniques erodes the effectiveness of traditional law enforcement prevention measures and reinforces the need for effective PAP measures.

While 9/11 emphasized the importance of installing security measures to guard against modern terrorist threats, private companies also have to prepare for natural disasters. Hurricane Katrina's devastating impact on industry in the Gulf Coast provided an alarming reminder of the vulnerability of private assets to natural disaster. Industry must ensure that terrorism preparedness is integrated with preparedness for other risks. Such an "all-hazards" planning approach is already common in the public CIP sphere and could be applied to support the development of comprehensive PAP security plans.³ For security providers that have traditionally worked in the CIP space, this provides an opportunity to translate their experience to the PAP market.

Shortcomings of Traditional Private Asset Protection Measures

Despite the escalation of threat and consequence, traditional facility security tools remain important. Terrorists and others seeking to cause harm tend to follow the path of least resistance. Even as target surveillance techniques grow more sophisticated, the

basics of deterrence still apply—visible security at doors, intrusion prevention and detection, surveillance, and weapons screening remain effective.

Exploitation of traditional security measures occurs normally not by circumvention of the tools themselves but rather by circumvention of the policies and procedures associated with those tools. One common procedural flaw is the dependence on compliance-based security assessments—the series of security checklists and step-by-step procedures used to simplify and codify security operations. This approach is useful in some situations, for instance, when training non-

Exploitation of traditional security measures occurs normally not by circumvention of the tools themselves but rather by circumvention of the policies and procedures associated with those tools.
 security employees in how to react to emergency situations. However, it is a dangerously weak overall security strategy, based on a cookie-cutter approach that fails to define desired levels of security performance, to measure overall effectiveness, or to integrate existing security systems and procedures.⁴

The biggest flaw of compliance-based security approaches is the stove-piping that occurs in relation to security policies, procedures, people, and technology. Disconnected security systems and processes lead to failures of both security and business operations. In some cases, lack of integration can cause security procedures to decrease overall security. This is particularly true when security is out of sync with corporate risk management strategies.

The compliance-based model exacerbates the flaws of traditional security measures, ranging from the physical protection of facilities and personnel to

security of information and due diligence of business partners and suppliers.

Facility Security

Guards and protective force personnel typically provide the first line of defense against intrusion. Security guards offer low-level protection that includes such services as closed circuit television monitoring, mail screening, inspections, and X-ray and canine screening. Highly specialized protective forces often

The biggest flaw of compliance-based security approaches is the stove-piping that occurs in relation to security policies, procedures, people, and technology

consist of former military and long-time law enforcement officers who receive intensive and continuous training to protect against a wide variety of threats. Additionally, response

teams can be quickly mobilized to provide assistance during disasters and crises.

As mentioned earlier, people who mean to do harm are sophisticated enough to analyze standard security procedures and plan against them. They may monitor and test facility and personnel vulnerability secretly for a long time before an attack to identify patterns and weaknesses in procedures, as well as human errors that may consistently undermine security. A common type of this “internal defeat” occurs when employees prop open doors for cigarette breaks.⁵

An additional weakness of compliance-based measures is that they are typically based on assumptions that may not be consistent with the threats and risks faced by the facility. For instance, a critical warehouse distribution center may be protected

against diversion, theft, and armed attack but remain wide open to simple disruption tactics, such as protesters laying in the middle of the only exit road. Because they often ignore the operational necessities of the facility, compliance-based security measures fail to anticipate predictable disruptions.

Surveillance Technologies

Complementary to physical security protection, and sometimes a substitute for protective forces, are surveillance and detection technologies. These include monitoring and surveillance equipment, access control systems, intrusion detection and alarm systems, and data protection. Security providers offer these services either on a stand-alone basis or as parts of an integrated system to match a company’s desired level of protection. Some providers offer fire detection, intercommunication systems, and enterprise management in addition to access control and security services.

Although typically touted as effective solutions to most security vulnerabilities, surveillance and detection technology is not a panacea. Even the most sophisticated intrusion detection system can be circumvented and/or exploited, particularly when the people, policies and procedures around them are weak. Explosive, metal, chemical, biological, and radiation detectors are useful, but only in the context of a strong overall security policy that prevents circumvention of devices by even “trusted” staff.

In fact, surveillance technology’s weakest link is its user. Monitoring and analyzing the raw surveillance data, and conducting counter-surveillance on potential threats, are not simple tasks—inadequate training and limited job experience have been identified as the most critical flaws in security effectiveness at airports and other facilities. In addition to provid-

ing sufficient training, surveillance operations managers must account for the physical and mental strain on security personnel asked to monitor multiple systems for hours on end. Finally, relying on people increases the importance of background checks and due diligence efforts to vet security staff and firms.

In the end, surveillance is a limited tool for security operations within a compliance-based system. While the technology itself may be working properly and procedures ostensibly followed, undetected malice and a natural level of human error can lead to significant vulnerabilities.

Information Security

Information security has received a great deal of attention from both business and government. Although the effectiveness of tools and procedures is tested continually (and sometimes with troubling results), one of the main weaknesses in current information security operations is the over-centralization of prevention and mitigation methods.

Information security tends to reside in a centralized system of controls emanating from the primary network. However, hackers and other outside intruders are more likely to take advantage of information security gaps by attacking distributed nodes—unsecured PDAs, mobile email devices, cell phones, laptops, and pass-cards—than by attacking the primary network. Information management is a critical weakness in both public and private information security schemes. Identity theft, phishing, dumpster diving, and social engineering are combined with widely available network cracking tools that require limited technical ability.⁶

Information security also has to account for all supply chain information threats. Companies need to understand the information security procedures their

downstream and upstream partners are using to determine if critical information is vulnerable through external nodes.⁷

In a compliance-based approach, information security is not integrated into other security measures, and sometimes is not even coordinated by the same security staff. If an isolated IT employee manages information security, physical security staff may not be aware of information security vulnerabilities or know how IT policies can limit the overall effectiveness of security measures.

Background Investigations

While the above measures are devised to keep potentially dangerous people from gaining entry into a facility or tapping critical information sources, private assets may also be threatened from people within the organization.

Most large firms, especially those trusted with sensitive and proprietary information, require prospective employees to consent to a credit check. Previous work history is often verified and, in many cases, attempts to verify trustworthiness end there. However, corporate espionage, theft of both real and intangible assets, acceptance of bribes and payoffs for proprietary information, and employee-assisted security breaches are prevalent, as was recently demonstrated by high-profile cases involving HP and Coca-Cola. They are also expensive: 43 percent of IT theft cases were perpetrated by insiders at a cost of about \$1.5 million per incident.⁸ Companies, such as government contractors and financial services firms, know from experience that credit and employment history checks are simply not enough to prevent or deter a desperate or greedy employee from acting against the interests of the company.

Background checks offer a deeper look into an

employee's past and offer employers a keener tool by which to judge applicants. In addition to verifying employment history, employers and acquaintances may be interviewed, education history confirmed, and court and criminal records examined. While first-time offenders may still prove difficult to identify, potential employees with patterns of criminal past behavior can be screened out. Additionally, similar services can be used, in conjunction with surveillance, to assist employers in identifying the source of information leaks or theft while an employee is still on the payroll.

In most cases, background checks are effective compliance-based tools for preventing workplace violence, theft, and other common incidents. However, whenever these checks are performed inconsistently or in breach of general security requirements—companies sometimes skip background checks when operational considerations, such as a desperate need to fill an important position, arise—their effectiveness declines.

Background investigations apply differently to different industries and to different units of the same company. In developing internal practices for background checks, businesses must take into account overall operational requirements and then insist on consistent implementation of adopted screening procedures.

Partner Due Diligence

All business partners and suppliers are potential weak links in the supply chain. Before relationships can be formed, firms must ensure the trust and reliability of their future partners and suppliers. Strict due diligence can identify partner vulnerabilities and isolate likely points of failure in the supply chain.

A standard practice with mergers and acquisi-

tions, due diligence also applies to temporary business relationships. Business practices, financial and accounting methods, past and current financial history, and any pending legal obligations involving a partner should be thoroughly evaluated.

Although 100-percent security is impossible, supply chain due diligence is an effective tool for reducing liabilities and for demonstrating to end customers a differentiated level of security. This is particularly important for government, and especially military, end customers. However, due diligence efforts cannot be assessed in a vacuum. It will be difficult to justify continual assessments of partners up and down the supply chain without consideration of operational realities and overall security and risk management.

Security Testing and Training

One final element to consider when assessing traditional security and risk mitigation measures is whether they are properly exercised. Few companies have tested their plans under stress and, therefore, can only estimate the function of their strategy in real time.

Employee training is the single most effective means by which to ensure safety in the event of an incident. Once physical security measures fail and a crisis occurs, response and evacuation plans are of no use if employees were never trained on how to implement them. While businesses in high-rise buildings conduct fire drills and offer evacuation training, most employees would not know how to respond to anything other than a fire.

Within a compliance-based security architecture, exercises are normally conducted according to the assumptions of the response plans. This type of security testing ignores the dynamic aspects of an emer-

gency and the interaction of plans during an incident. For instance, a fire drill will normally not consider options available in the case of severe weather that impedes evacuation, man-made fires that portend other violence against evacuees, fire that occludes evacuation routes, or other disruptions that could increase panic and disrupt the evacuation plan. The same lack of plan integration extends to continuity of operations plans (COOP) and other important tools for post-incident recovery.

A Model for Organizational and Supply Chain Resiliency

While the above security measures have individual merit, all are vulnerable to potential system failure. Each security component relies on the idea of compliance: personnel investigators will be thorough; monitors will never look away from the screen; partners will maintain financial integrity; employees will respond exactly as they are trained. Reliance on individual security measures without consideration for

how these measures should interact with each other is problematic. Under pressure from natural disasters or direct circumvention by terrorists or criminals, systems are likely to fail at some point.

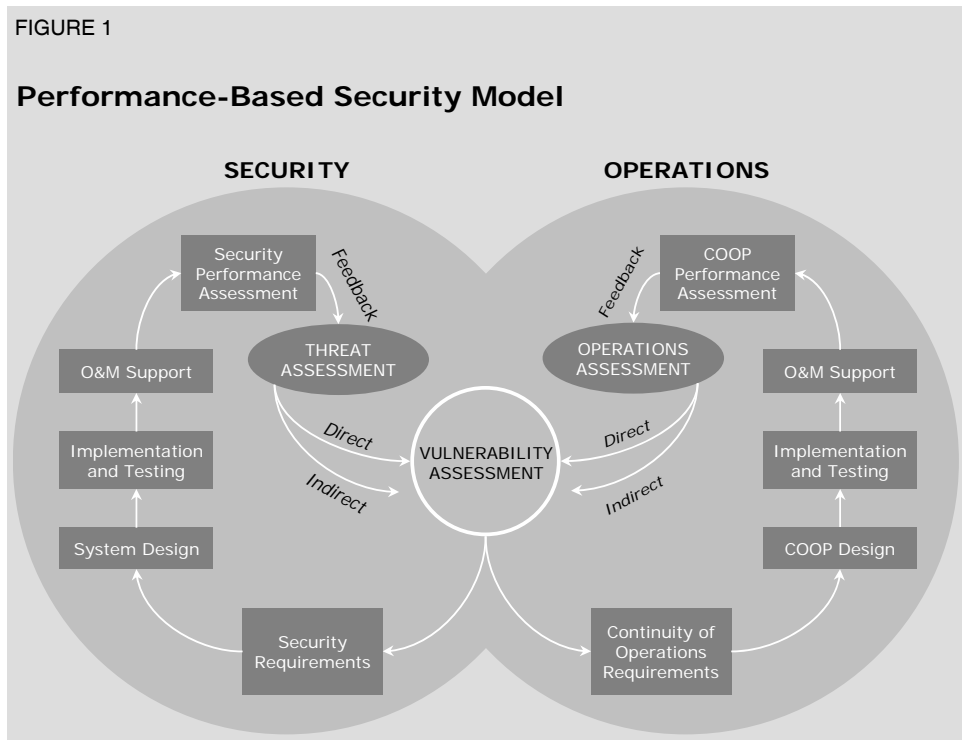
Moreover, the cost of implementing rigorous detection schemes and using the most sophisticated equipment may be prohibitive for many companies. While there is not always going to be a cost-benefit calculation to support significant expansion of security measures, companies often neglect certain paths to an outcome worthy of security spending.

Performance-Based Security

Outcome-oriented, performance-based security measures attempt to mitigate the impacts of an incident or disaster by enhancing the organization’s resiliency. These measures minimize effects on overall operations and facilitate rapid recovery after an incident. Meanwhile, COOPs ensure that the essential functions of a business are protected during a disaster. Achieving organizational resiliency through careful

planning and foresight is critical to ensuring the integrity of the chain of command and all crucial information.

A performance-based model focuses on the outcome to be prevented, not on the attack method. Having defined all potential hazards and threat objectives, the model then works backward through all the pathways leading to the undesired outcome. When properly implemented, performance-based models are more adaptable to outside threats than compliance-



based methods. More importantly, they can significantly lower costs by streamlining technology solutions, optimizing security personnel, and mitigating multiple threats simultaneously.

The performance-based security model draws on a systems engineering design and has three essential analytical components: threat assessment; operations assessment; and vulnerability assessment (see figure 1).

Threat or risk assessments focus on external threats or risks affecting assets, people, information, and infrastructure. They cover both direct threats (targeted at the company) and indirect threats (targeted at some other component of the supply chain).

Operations assessments seek to capture internal operational weaknesses within the supply chain, to include receipt of material from suppliers, day-to-day value-added operations, and delivery of goods and services to customers. Similar to threat assessments, operations assessments address both direct risks (emanating from purely internal operations) and indirect risks (external components of the supply chain).

Finally, vulnerability assessments aim to combine the two preceding processes. A company can identify disruptive outcomes in an operational assessment and map them back to potential threats and risks. Vulnerabilities are then assessed by both impact and likelihood, paying particular attention to single points of failure, primary and operational functions, high-probability threats, and low-probability, high-consequence events. Vulnerability assessments are critical risk management tools that direct decisions about how much external and internal risk can be tolerated from security and operational perspectives.

Vulnerability assessments enable the develop-

ment of interlocking security and operations requirements. These requirements inform the design of security systems and COOPs, with a focus on facility, people, technology, and policy considerations. These are best codified in requirements documents that clearly spell out the linkages among the vulnerability assessment, risk tolerance, tolerance for disruptions to operations caused by security measures, and desired security and operational outcomes.

A particularly important component of security and continuity of operations is continual assessment of performance. Performance measures should be tied to fulfillment of security and operational requirements and to compliance with practices and policies specified by the systems and plan designs. This means that both qualitative and quantitative assessments must be developed and periodically administered. Feedback from these assessments should be filtered into the next round of threat/risk and operations assessments.

A rigorous and frequent series of table-top, functional, and full-scale exercises that examines procedures and policies will expose and correct weaknesses before they can be exploited. Rigorous testing procedures will not solve every problem, but they teach adaptability in the face of a crisis and provide much better feedback than the execution of static drills. Ultimately, what makes performance-based security models effective is full integration of security policies, people, and technologies with security requirements and operational considerations.

The Role of Integrators

Performance-based security measures integrate all aspects of security to eliminate the dangerous gaps among people, process and technology that can grow in traditional compliance-based security systems.

Complete integration often is missing in current offerings. No single security provider offers the entire menu of services a supply chain manager requires. Current bundling of security offerings is inadequate to meet all business and supply chain security requirements.

The large degree of overlap among sectors of the security services market, the complexity of customer requirements, and the growing number of providers create a role for systems integrators. In the past, systems integrators catered primarily to the public sector, especially the federal government, with services and products that included access control measures, intrusion detection and perimeter protection. Today, cross-cutting technologies find increasing application to both public infrastructure and private asset protection. As supply chain managers turn to integrated security solutions, they adopt the technology and processes that were once exclusive to public infrastructure security.

With technology constantly evolving, integrators are required to incorporate new solutions into old security systems. Biometrics, radars, and HAZMAT systems are examples of this new approach toward comprehensive security. As robotics, sensors, and more robust command and control systems are developed and security systems become more performance-based, systems integrators will be critical to ensuring that all these innovative technologies fit into a comprehensive security framework. Companies without integration capabilities and those that fail to demonstrate their value to end customers are going to be at a disadvantage as this market develops.

Toward an Integrated Security Market

As integrators become more important to the implementation of performance-based security measures,

many traditional PAP providers will find both new competition and potential partners in companies from the public CIP space. Likewise, defense contractors looking for new markets should look at these integrator opportunities as a way to diversify their current customer base.

Several strategies are available to security providers eager to improve their competitiveness in the integrated security market. Which strategy they adopt will depend on their capabilities, past performance, and available investment resources. In some cases, a combination of strategies may be most appropriate.

Leverage Adjacent Market Competencies

Companies that are new to the PAP market should leverage adjacent security competencies. Depending on the company, these may include public facility security, CIP tools, force protection of military bases, or high-level systems integration. These capabilities are difficult for traditional players to develop organically and are therefore valuable differentiators in the integrated security space.

While this adjacent market experience may reduce the cost of market entry, it will not necessarily translate into contracts. In most cases, firms will have to develop new competencies before achieving a truly competitive market position. This may mean investment in assessment and intelligence capabilities, or acquisition of additional security technology integration expertise.

Develop Core Market Competencies

One strategy to stay competitive in the PAP market is to develop organic capabilities. This usually entails hiring subject matter experts while simultaneously investing resources to expand the capabilities of existing personnel and business units.

Internal investment strategies can avoid the cultural clashes and capability disconnects that often accompany acquisitions. However, the investment required by companies can be substantial, and a properly implemented strategy requires long lead times, typically 18–24 months, to bear fruit. Expectations for enhanced business development can be very high, and asking too much of an embryonic organization can lead to disaster.

Partnerships and Joint Ventures

Another potential strategy is to pursue strategic partnerships (both formal and informal) that allow companies to combine capabilities to leverage synergies and offer comprehensive service packages. This strategy is particularly attractive to companies that occupy a healthy market position and need to fill capability gaps or to smaller providers looking to increase their market visibility.

The advantages of this strategy include short time to market for new services and minimal investment in new technology. The combination of two “name-brand” organizations may also offer cross-marketing opportunities.

Though attractive on paper, partnerships do not always deliver the value they seem to promise. Dissatisfaction and disparate expectations can cause arrangements to sour. The inherently stove-piped arrangement of most partnerships and joint ventures often impedes integration of security solutions. As a result, many partnerships fail to deliver the synergistic value they sought early in the relationship.

The advantages of partnerships make them strong interim stop-gap strategies for companies considering other organic and inorganic strategies, but firms should approach them with sensible caution.

Mergers and Acquisitions

Finally, companies may attempt to acquire the competencies and experience required to be competitive in the integrated security market. An acquisition strategy would be attractive to companies with adjacent market experience but lacking PAP market presence, as well as to larger traditional PAP players in need of complimentary capabilities that a smaller supplier can provide.

An acquisition or merger can offer immediate access to capabilities, customers and contracts—a major advantage over other strategies. However, such a move should not be taken lightly. Apart from the significant financial risks, the wrong acquisition can saddle a company with a market position or a set of competencies that undercut its overall market poten-

TABLE 1

Strategic Options for the Integrated PAP Security Market

STRATEGY	TYPE	PURPOSE	ADVANTAGES	DISADVANTAGES
Leverage Adjacent Competencies	Organic	Leverage capabilities in other markets, such as CIP, system integration, or construction experience as the basis for a market entry strategy	Providing a basis for market entry and experience could prove valuable to another provider looking for partnerships or acquisitions	Need to be combined with one of the other strategies to be effective and therefore has the disadvantages of the strategy chosen
Develop Core Competencies	Organic	Invest in internal development of differentiated core capabilities	Optimized integration of capabilities and best leveraging of core market position	Longest lead time, modest financial risk, and requiring some degree of market incumbency
Partnerships and JVs	Inorganic	Fill gaps in competencies and market presence through formal relationships with other providers	Minimal financial risk and rapid access to new capabilities	Sub-optimized integration inhibits synergies and ultimately undercuts its value proposition
Mergers and Acquisitions	Inorganic	Fill in gaps in competencies and presence through adding people and institutional experience	Rapid access to new capabilities and ability to buy established market share and knowledge	Significant financial risk and long lead time for optimal integration of new company, people, and services

tial. While an acquisition strategy can allow immediate expansion of current capabilities, it may take months or years to fully integrate acquired experience and capabilities.⁹

Conclusion

Five years after 9/11, protection of private assets and infrastructure remains less than satisfactory, relying on traditional security measures and stand-alone solutions. With government homeland security and force protection budgets increasingly constrained, a growing share of the burden for implementing new security measures will fall on the private sector.

Security providers that can demonstrate the value of integrated security within an enhanced performance-based risk management framework will have a distinct advantage in this market. While supply chain managers will be compelled to move to performance-based strategies, translating that strategy into a truly integrated system will require security providers to invest in new capabilities.

There is no strategic silver bullet for entering or growing share in the PAP market. Choosing the right strategy requires a thorough understanding of PAP market fundamentals including customer priorities, technology trends, future requirements, and competitive barriers. A first step for firms considering

entry into his market is to inventory internal capabilities and reevaluate their ability to play in a changing security environment. ▼

¹ See in this issue “Mapping and Assessing Security Threats Across the Supply Chain.”

² See, for example, the translation of “Military Studies in the Jihad Against the Tyrants” (a.k.a. The Al Qaeda Manual), an alleged training document seized in 2000 in the UK as part of the investigations into the 1998 US Embassy Bombing in Kenya. Excerpts are available at the US Department of Justice Web site, www.doj.gov.

³ For a basic history of all-hazards planning in emergency management, see Lloyd Bokman, “All-Hazards Planning: What Does It Mean?” *Natural Hazards Observer* 27, No. 4 (March 2003), www.colorado.edu/hazards/o/archives/pastobservers.html (September 10, 2006).

⁴ See Howard L. Borst and Clifford A. Lewis, “Systems Effectiveness Assessment (SEA) Process: A Performance-based Methodology for the Design & Evaluation of Physical Protection Systems,” Presentation to the 18th NDIA Security Division Symposium & Exhibition, June 26, 2002.

⁵ For more examples and other limitations of security systems, see Fred Burton, “Corporate Security: The Technology Crutch,” *Stratfor Weekly*, August 2, 2006, www.stratfor.com (September 10, 2006).

⁶ Kyle Schurman, “The Dark Side Of Scripts,” *Smart Computing* 6, No. 6 (June 2002): 173–176

⁷ For more information, see Michael Johnston, “The Information Supply Chain: Data Integrity Rises in Stature,” *Supply Chain Management Information Portal*, March 22, 2005, <http://scm.ncsu.edu/public/security/sec050322.html> (September 10, 2006).

⁸ Kelly Jackson Higgins, “Study: Rethink the Outsider Threat,” *DarkReading*, August 28, 2006, www.darkreading.com (September 10, 2006).

⁹ See Daryle E. Lademan et al, “Deal or No Deal?” and Nicholas C. Howland and Mark Shields, “Beyond the Deal,” *The Avascent Review*, No. 11 (June 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.