

Protecting the Public From Supply Chain “Evils”

Mitigating Risks and Attacking Vulnerabilities



by

Jim Beggs

beggs_james@bah.com

Craig Fitzpatrick

fitzpatrick_craig@bah.com

Charles Gardner

gardner_charles@bah.com

Booz | Allen | Hamilton

delivering results that endure

Protecting the Public From Supply Chain “Evils”

Mitigating Risks and Attacking Vulnerabilities

Traditionally, government agencies and private sector companies have recognized the need to make their supply chains more resilient. This increased resiliency helps prevent the risk of disruptions caused by unfortunate events, such as natural disasters or terrorist attacks. The aim of resilience is the continuity and effectiveness of a supply chain under adverse conditions.

More recently, government organizations have begun to understand the challenges presented by two very different supply chain scenarios. In both cases, the government aims to protect the public from adverse impacts (“evils”) created by or in a supply chain. The first case involves the illicit use of supply chains. By attacking these supply chains, the government can slow or stop the movement of illicit goods, such as drugs or weapons. The second case involves the introduction of contaminants—accidentally or deliberately—into otherwise beneficial supply chains. Examples include food-borne disease, lead, and cyber threats. To protect the public in the second case, the government must quickly identify and stop the source of the contaminant while simultaneously tracing the path of contaminated products to prevent further harm to the public.

Booz Allen works with clients to address all three of these issues—building more resilient supply chains to withstand disruptions, disrupting harmful or dangerous supply chains, and protecting against harmful contamination entering supply chains. This paper provides an overview of client challenges and how our capabilities can help organizations achieve the mission of protecting the public from supply chain evils.

Supply Chain Resilience—Preparing Organizations to Bounce Back

Supply chain resilience has come to the forefront in recent years. Numerous examples illustrate the severe disruption that occurs when commercial companies and government organizations fail to plan for these

types of events. History contains many examples of both manmade and natural disasters that have led to supply chain disruptions. Full-scale inspections at border crossings after the terrorist attacks of 9/11 created catastrophic production delays for auto manufacturers depending on just-in-time component deliveries. Hurricanes have shut down supply sources for entire industries (e.g., bananas—Hurricane Mitch, 1998; oil, natural gas, and chemical production—Hurricane Katrina, 2005). Union strikes in a supplier base have also crippled companies and entire industries. British Airways (BA) suffered costly losses when its ground employees’ union staged a 1-day strike after a BA dispute with a catering supplier in 2003. The threat of a west coast longshoreman’s strike and temporary lockout in 2002 cost retailers and manufacturers billions.

Booz Allen has a well-developed service offering to help clients make their supply chains more resilient. By taking an integrated, end-to-end view, we are able to work with clients to find weaknesses in a given supply chain and develop strategies for reducing the risk of a catastrophic failure.

Protecting the Public—Understanding Supply Chain “Evils”

Although supply chains are recognized as important contributors to our daily lives and our business success, less recognized is the fact that supply chains can also have a negative impact on our society. The negative impacts of supply chains can transpire in two ways.

The first undesirable supply chain impact is the role of supply chains in illegal trafficking. For example, drug trafficking organizations have developed elaborate and highly resilient supply chains to deliver illicit products to their markets. Likewise, traffickers of weapons, illicit nuclear materials, persons, illegal immigrants, and materials used to construct explosive devices

have developed sophisticated supply chains to both obtain and deliver their contraband. By understanding adversary supply chains and their vulnerabilities, government agencies have an opportunity to slow or stop the flow of illegal goods. Booz Allen is at the forefront of this emerging area and is currently working with federal agencies to shape the US government's thinking and approach.

A second undesirable impact of supply chains involves supply chains that become conduits for contaminated products—whether deliberately or accidentally. Recent examples are melamine in milk, salmonella in peanut butter, and lead in toys. In a similar vein, concern exists about the infiltration of cyber networks with chips or other components containing deliberately planted malicious software, which could be used for spying, operational disruption, or—even worse—sabotage. Government agencies with responsibility for protecting the public from these dangerous and life-threatening hazards face simultaneous challenges. First, they must find and stop the source of the contamination; then, they must discover how far the contaminated products have progressed in the supply chain in order to remove them and protect the public from further harm. The government's ability to establish more effective prevention would be an even greater achievement.

In working with and discussing these issues with government clients over the past year, we have determined that our supply chain resilience methodology can effectively protect the public from harmful supply chains. Just as we have observed the catastrophic effects that occur when a supply chain is unprepared to deal with disruptions, we can identify vulnerabilities to create disruptions and cause cascading failures in illicit supply chains. At the same time, our ability to quickly analyze and generate an integrated, end-to-end view of a supply chain enables us to isolate sources of contamination in friendly supply chains and track the flow of contaminated products.

In both harmful supply chain scenarios—protecting the public by mitigating risk and disrupting the illicit use

of supply chains—our approach supplements rather than replaces our clients' existing capability, bringing a unique perspective. The aim of our approach is to provide a joint capability that continuously monitors, assesses, and develops strategies for the respective supply chains as new conditions arise.

Illicit Use of Supply Chains—Attacking Vulnerabilities

To address illicit trafficking, Booz Allen works with clients to develop attack strategies. That is, we reverse engineer the supply chain to find weaknesses that we can attack in the illicit supply chain to cause disruption. Not only can we identify weaknesses with cascading impacts for significant time periods but also we can anticipate what the traffickers' remedial actions will likely be to further enrich our attack strategy.

The key elements of our approach involve understanding the supply chain from end to end. We examine every aspect of the product supply chain—from raw materials and multi-tiered suppliers to manufacturing, storage, handling, distribution channels, transportation, inventory strategy, wholesale, and, ultimately, retail distribution to customers. We can also apply these frameworks in both directions. For example, analyzing the reverse supply chain which involves understanding the movement of cash or contraband items that participants can use to launder cash.

In these situations—particularly the illicit use of supply chains—we do not typically find well-documented shipping records, revenue flows, or sales-demand data. Instead, we often rely on intelligence reports, capture and interdiction reports, and other case information. Law enforcement and intelligence agents focus on the command and control structure within criminal enterprises. Therefore, the case files and intelligence reports tend to be organizationally focused, rather than process focused as is typical in an operational supply chain analysis. Our approach is to translate existing bodies of knowledge through interviews with knowledgeable agents and database analysis into a process oriented supply chain framework. In

this manner, our experienced supply chain experts have found the data and information to be extremely analogous to supply chains we have seen in countless legitimate businesses.

We have also seen organizational structures that we can match against very successful logistics operations in the commercial sector. We have seen highly resilient supply chains driven by the need to minimize risk of seizure. We have seen the adaptations performed by very clever logistics operators to make their supply chains resilient in the face of persistent and increasing adversity. Nevertheless, we also see very apparent weaknesses that have not yet been exploited.

A successful supply chain attack framework begins with a robust identification of risks. This process uses a holistic view of supply chain operating units and functions to uncover shared risks in the supply chain and to uncover the risk management strategies already in use. For example, supply chain operators anticipate attempts to interdict and seize their illicit cargo. As a result, they greatly diversify routes and modes of transportation, limiting the opportunity for their adversaries to capture significant quantities of product. Although this diversification is costly and inefficient, these operators view it as the cost of doing business. Meanwhile, interception of the illicit cargo in transit becomes a very expensive and ineffective attack strategy. Although interception does raise illicit traffickers' risks and costs, it is very difficult to intercept more than a small percentage of shipments. A more effective approach involves identifying and attacking the operators who organize and orchestrate those shipments. These operators rely on mutually trusting relationships and specific skills to manage the totality of shipments across multiple lanes and modes. By removing the supply chain operator in this collaboration, we can significantly disrupt the flow of illicit goods.

Supply Chains—Mitigating Dangers

To address public health and information security threats, Booz Allen works with clients to quickly mitigate dangers. We use our supply chain resilience

methodology to more quickly and effectively identify the source of contamination and trace its distribution in the supply chain to prevent further impact.

As we examine dangerous events in supply chains, similar considerations apply. However, we must also understand the stage of crisis at hand. That is, has a form of contamination already occurred, or does an opportunity to prevent a crisis remain? Unfortunately, in the case of contamination, it is all too likely that an issue is discovered because the impact is already in effect, people are becoming sick from the contamination, or networked information systems have been severely disrupted. At that point, the focus must be both upstream and downstream in the supply chain. We must find the source and eliminate it (upstream) and head off further harm (downstream).

Pre-crisis, we work with our clients to consider more effective inspection and monitoring approaches, as well as more effective regulation, to better prevent dangers from entering a supply chain.

It is important to note that Booz Allen couples its approach with appropriate public health and epidemiological partners or their equivalent in other scenarios. We do not have the ability to test for or determine cause of disease. However, our approach assists these practitioners with more quickly identifying the likely path of the contamination in the supply chain. Bringing supply chain expertise to bear allows public health and other experts to focus their energy on their own analytical strength. Our supply chain experts provide a more holistic, end-to-end view of the problematic supply chain, often cutting across regulatory agencies' organizational boundaries. This end-to-end view can illuminate multi-tiered processes and flows that might otherwise escape scrutiny.

Although it is important to minimize downstream risk, an uninformed view of the supply chain can lead to a broad-brush approach (e.g., recalling all products even remotely associated with the contamination). The impacts of such broad-stroke actions may indeed minimize risk but may do so at the cost of shutting down major segments of an industry. In the cyber

scenario, a similar broad-stroke approach to minimizing network risks could have unacceptable consequences for other key operations.

How Booz Allen Can Help

Whether to exploit or minimize the risk of a supply chain weakness, our supply chain risk and exploitation framework culminates with an analysis of both likely impact and degree of difficulty to attack or apply corrective measures. Along the way, we prioritize and measure risks to provide the basis for effective strategies.

The benefits to government organizations charged with protecting the public include more powerful tools to accomplish their missions. By focusing on end-to-end supply chain flows and functions, Booz Allen helps agencies—

- Gain a more holistic perspective of how to resolve key issues with major supply chain components
- Gain insights based on an integrated, end-to-end supply chain view; this view is difficult to achieve using historical approaches to the same challenge
- Focus the agency's expertise and energy on its own core competency, positioning the agency for greater effectiveness with our supply chain expertise
- Cut across internal, inter-department, and inter-agency organizational boundaries
- Better interpret existing data and identify more useful data to collect
- Identify, test, and implement mission strategies with greater impact and efficiency
- Establish a cell to continuously monitor, assess, and develop effective strategies as supply chain conditions change and evolve.

About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for nearly a century. Today, Booz Allen is a leading provider of management and technology consulting services to the US government in defense, intelligence, and civil markets, and to major corporations, institutions, and not-for-profit organizations. In the commercial sector, the firm focuses on leveraging its existing expertise for clients in the financial services, healthcare, and energy markets, and to international clients in the Middle East. Booz Allen offers clients deep functional knowledge spanning strategy and organization, engineering and operations, technology, and analytics—which it combines with specialized expertise in clients’ mission and domain areas to help solve their toughest problems.

The firm’s management consulting heritage is the basis for its unique collaborative culture and operating model, enabling Booz Allen to anticipate needs and opportunities,

rapidly deploy talent and resources, and deliver enduring results. By combining a consultant’s problem-solving orientation with deep technical knowledge and strong execution, Booz Allen helps clients achieve success in their most critical missions—as evidenced by the firm’s many client relationships that span decades. Booz Allen helps shape thinking and prepare for future developments in areas of national importance, including cybersecurity, homeland security, healthcare, and information technology.

Booz Allen is headquartered in McLean, Virginia, employs more than 25,000 people, and had revenue of \$5.59 billion for the 12 months ended March 31, 2011. *Fortune* has named Booz Allen one of its “100 Best Companies to Work For” for seven consecutive years. *Working Mother* has ranked the firm among its “100 Best Companies for Working Mothers” annually since 1999. More information is available at www.boozallen.com. (NYSE: BAH)

To learn more about the firm and to download digital versions of this article and other Booz Allen Hamilton publications, visit www.boozallen.com.

Contact Information:

Jim Beggs

Principal

beggs_james@bah.com

703-377-0837

Craig Fitzpatrick

Senior Associate

fitzpatrick_craig@bah.com

202-346-9018

Charles Gardner

Lead Associate

gardner_charles@bah.com

703-984-3076

Principal Offices

Huntsville, Alabama	Indianapolis, Indiana	Philadelphia, Pennsylvania
Sierra Vista, Arizona	Leavenworth, Kansas	Charleston, South Carolina
Los Angeles, California	Aberdeen, Maryland	Houston, Texas
San Diego, California	Annapolis Junction, Maryland	San Antonio, Texas
San Francisco, California	Hanover, Maryland	Abu Dhabi, United Arab Emirates
Colorado Springs, Colorado	Lexington Park, Maryland	Alexandria, Virginia
Denver, Colorado	Linthicum, Maryland	Arlington, Virginia
District of Columbia	Rockville, Maryland	Chantilly, Virginia
Orlando, Florida	Troy, Michigan	Charlottesville, Virginia
Pensacola, Florida	Kansas City, Missouri	Falls Church, Virginia
Sarasota, Florida	Omaha, Nebraska	Herndon, Virginia
Tampa, Florida	Red Bank, New Jersey	McLean, Virginia
Atlanta, Georgia	New York, New York	Norfolk, Virginia
Honolulu, Hawaii	Rome, New York	Stafford, Virginia
O'Fallon, Illinois	Dayton, Ohio	Seattle, Washington

The most complete, recent list of offices and their addresses and telephone numbers can be found on www.boozallen.com by clicking the "Offices" link under "About Booz Allen."