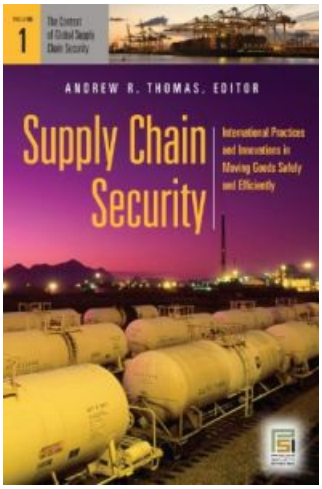

Book Supply Chain Security

International Practices and Innovations in Moving Goods Safely and Efficiently

Andrew R. Thomas
Praeger, 2010
Listen now

- play
- pause

00:00
00:00

Recommendation

Everyone talks about globalization, but almost no one ever discusses the gritty details about how goods actually move around the world. This two-volume set changes that situation with 24 comprehensive essays on international best practices in supply chain security. The first volume deals with "The Context of Global Supply Chain Security," and the second volume covers "Emerging Issues in Supply Chain Security." These collections of thorough, practical, well-written articles by leading experts in security, crime prevention and logistics cover a range of issues and detailed information from legal exposure and risk assessment to supply chain management. They include specific precautions for those involved in transporting goods worldwide by air, road, rail and sea. These essays are focused, revealing and fully documented with citations and bibliographies. While some chapters are redundant and technical, this is a worthwhile, unusual and timely package of deeply informative books. *BooksInShort* highly recommends it to global supply chain managers, shipping industry practitioners and their clients, and anyone concerned about the compounding, disruptive effects of terrorism and crime on a global economy. (And if you're a terrorist or an international cargo thief, just forget these inside prevention tips, OK?)

Take-Aways

- Due to theft and fraud, 15% of goods shipped worldwide do not reach their destination.
- Supply line thieves take advantage of weak security, poor auditing, fake documents, inadequate technology and fraudulent payments.
- eBay employs 2,000 fraud investigators to stop crooks selling stolen goods on its website.
- Counterterrorism strategies focus on increasing detection, reducing the possibility of an attack and minimizing the negative impact of a successful assault.
- In the US, 13 federal departments, administrations and agencies provide supply chain security measures to combat terrorism.
- Between 1968 and 2007, terrorists conducted 24,000 attacks, 1,267 of them aimed at land-based mass transit and more than 30 aimed at aircraft.
- Pirates attacked 122 ships in 2008, seized 42 and demanded ransoms in the millions.
- The shipping industry must coordinate with security agencies to prevent attacks against it.
- Special security provisions address the needs of air cargo systems, oil pipelines, ports, railways and trucking. Climate change may necessitate new security measures.
- The entire supply chain is only "as strong as its weakest link."

Summary

Supply Chain Theft

Theft is all too common in business, from outright stealing to online schemes to the purchase of stolen goods. To complicate the problem, thieves commonly use

legitimate channels to ship and sell stolen merchandise, including guns, drugs, and counterfeit goods. Each year, criminals steal about $50 billion in goods worldwide at various points along the supply chain. Theft is even more likely when manufacturers ship goods directly or send them through complex supply lines, when items are stored in poorly secured areas, and when high market demand boosts the profit potential for selling stolen goods.

> "The 'supply chain' encompasses all the links connecting a manufacturer to end users of its products."

In practice, a "cross-dock" theft operation can work like this: Thieves take a stolen shipment to a public warehouse and unload the merchandise. This gives them a distribution and transit point, and it enables them to establish a new "phantom" carrier with a clean bill of lading. The thieves then hire freight firms to redistribute the merchandise. Legitimate carriers have no way of knowing about the switch. In some cases, thieves mix stolen merchandise with legal goods, which further complicates the verification process. At this point, the stolen goods move from the underground economy to the main stream.

> "As supply chains and operations are globalized, they become increasingly complex, dynamic and interdependent across multiple suppliers located in multinational geographic locations."

Kroll Associates' 2007-2008 "Global Fraud Report" estimated that 42% of firms worldwide had experienced at least one incident of theft or supplier fraud, or both. "The economic impact of cargo theft" amounts to 1% of the United States' gross domestic product, and "cargo and supply chain theft" equal nearly 1% of global gross national product. The sale of stolen goods is so common that eBay employs 2,000 people to investigate fraud and to find fencers who are selling hot goods on its website. Tracking theft is complex due to systemic ambiguity about responsibilities and payments associated with insurance claims, damage to reputation, recovery times, and storage, thus most industrial supply chain thefts go unreported. Ironically, retail stores spend more time and money on preventing shoplifting than on protecting their supply chain.

> "The sophistication and business skills involved with managing an international criminal enterprise is equal to any international importer in any country."

Criminals also use altered documents and take advantage of poor auditing, inadequate technology, and fraudulent payments. Despite international efforts, the growth rate of international cargo theft is not falling, and thieves have adopted more violent tactics. In Mexico, Russia, Brazil, South Africa and the UK, the number of violent cargo crimes has increased. Theft of unattended cargo is up in the US, where thieves take billions of dollars in goods annually from trucks and containers. These costs eventually end up on consumer price tags. One estimate says the cost of goods stolen from the supply chain amounts to $50 a year for every American. The computer industry adds $100 to each unit for loss coverage. This problem proliferates because insurance firms don't make policyholders increase antitheft protection or adopt preventive technologies.

Security and Terrorism

Terrorism is the threat or use of violence for political purposes. Security experts evaluate and prioritize terrorism-related threats in terms of their probability and ramifications in order to focus governments' limited defense resources. Between 1968 and 2007, terrorists staged 24,000 "incidents," including 1,267 attacks on land-based mass transit and more than 30 attempts against aircraft. Starting with the 1968 hijacking of an El Al flight to Italy, terrorists use their deadliest attacks against planes, either smuggling explosives onboard planes or firing ground-to-air missiles, sometimes with fatal consequences.

> "Since most industrial and supply chain theft is unreported, specific data does not exist."

Commercially, some 60% of global trade and 95% of the US's foreign trade is oceangoing, making violent piracy a popular, increasingly frequent criminal activity, particularly in waters near Somalia, Nigeria, Bangladesh, Kenya, and the Philippines. In 2008, pirates – who succeed in taking ships in about 75% of their attacks – went after 122 vessels and demanded ransoms from $1 million to $3 million to release the ships. These pirates often held ships captive for months, and that year, they extorted $40 million from shipping companies. The UN Convention on Maritime Law allows policing actions against pirates, but ship owners generally pay ransoms and do not tell authorities or their insurance companies so their rates will not soar.

> "A cultural change is needed to begin the process to protect cargo, business assets and profits for all concerned."

The US criminalized piracy in 1790, and many other nations have done the same, but pirates find sanctuary in lawless nations like Somalia, whose waters provide safe harbor near busy trade routes like the Gulf of Aden, a transit point for an estimated 21,000 ships a year. To avoid conducting apparent acts of war, the US Navy cannot blockade ports in nations that don't seek its help. Alas, some countries do little to protect their vessels or to capture pirates, and maritime laws often conflict or leave questions unanswered; for example, who is responsible if pirates sink the ship and its cargo? Many governments lack the political will to battle piracy, contending that capturing these criminals could violate their human rights. The world needs new international laws and coalitions to combat this growing problem.

Practical Applications

To raise the shipping industry's level of counterterrorism prevention, management and security must be in sync. Supply chain managers should collaborate with their buyers about shared and individual risks. Large manufacturers and suppliers, such as Procter and Gamble, and retailers, like Target, formed strategic collaborations. For instance, corporations now collect data at the point of sale to identify risk levels in specific countries, industries and companies; such information also helps firms accelerate production and transport.

> "All of these criminal acts are defined as theft, for they erode corporate profitability, put users at risk and dramatically affect the economy."

Companies must combat terrorism and crime because – due to its vast complexity – the entire supply chain is only "as strong as its weakest link." Among other steps, firms can offer continual training to teach their employees how to detect potential terrorism or crime. Companies also should monitor intelligence sources. Approximately 95% of all information on counterterrorism is available from the private sector and universities, so the shipping industry is not dependent only on government data. Criminal networks constantly change their methods and seek new opportunities, creating an environment of perpetual upheaval where everyone involved in protection must stay abreast of developments. This makes places with standardized regulations (such as the European Union) more vulnerable to penetration by criminal or terrorist gangs.

"In some nations, bribes are an accepted method of opening trade negotiations, but American law prohibits American companies from giving bribes."

Supply chains risks can occur anywhere along the route connecting manufacturers and distribution facilities. In a complex operation – for example, supplies moving into a General Motors (GM) plant and cars moving out – the chain is tangled, following multiple paths among its networks and tiers of suppliers and dealers. Researchers use various risk assessment tools, such as probability distributions, to track risk, not only from terrorism or theft, but also from weather, natural disaster, fire, or labor strikes.

"If the truth be known, ransom has been paid many times unbeknownst to the [victims'] states or the United Nations."

When analysts examine all possible risks and their possibility of playing out, they use a "comprehensive probability distribution" process called "convolution." This risk analysis, which establishes a range of prospective monetary loss, involves very complex computations due to the number of variable inputs, such as the quantity of disruptive events and their individual effects on a multifaceted operation. For example, GM has identified 26 possible geographical disruptions to its "physical flow of goods" that could affect its 139 plants worldwide. That gives a total of 3,614 possible supply chain disruptions. To track the impact of just one such disruption, consider what happened after a small fire damaged a factory that sold chips to telecommunications giant Ericsson. Workers extinguished the fire in 10 minutes, but it caused a power failure, letting smoke and water enter the "clean room." The plant took six months to rebuild production to just below 50% of its previous level. Within a year, Ericsson posted a $200 million net loss, mostly due to this fire. The firm told employees that "everyone is a risk manager." Supply chain breaks are even more disruptive in plants that rely on just-in-time inventory management.

Measuring Performance and Impact

The goal of any program that measures protection or performance is to change the way individuals and teams behave. Counterterrorism strategies should focus on lessening the possibility of attacks, reducing damages to important assets, increasing the likelihood of detection and minimizing the negative impact if an attack succeeds.

"The understanding of how an event will take place and how to respond is not intuitive, but can be learned."

To achieve these goals, various agencies have created systems to enhance security and expedite the transfer of goods. A multilayered group of governmental and private agencies combats supply chain security breaches. In the US, the Department of Homeland Security sits at the top of the ladder. No less than 13 protective federal departments, administrations, and offices enforce security directives and regulations. For instance, the US Customs and Border Protection Agency runs the voluntary Customs-Trade Partnership Against Terrorism Program that evaluates supply chains to allow some companies to classify their shipments as "low risk." More than 900,000 workers have qualified for the Transportation Worker Identification Credential. Supply chain locations are now under increased video surveillance.

"As the [Irish Republican Army] famously stated to British authorities, 'We only have to be lucky once – you have to be lucky all the time'."

The best practices for ensuring business continuity and restoring the flow of goods after an emergency involve planning and partnerships between private and public groups. This includes employee transportation (one West Coast company has arrangements with a local taxi company), evacuation procedures, and ways for employees to telecommute while offices are closed. In Washington, DC, hotels managers meet regularly with government officials to run through various disaster scenarios, including lodging for personnel the government would need to maintain operations. Some companies have crisis notification systems based on text messaging, phones, satellite mapping systems and email. New York City has a Corporate Emergency Access System, while California's Genentech preregisters key workers with local government officials so they can be admitted to restricted areas in the event of a crisis.

Other Transportation Facilities

A security plan should also encompass air cargo, port and trucking security:

- **Air cargo security** – Air cargo companies can hire security-certified freight handlers, reputable shippers and "regulated agents." However, this system works only if participants maintain exacting criteria and security standards. To join the US Known Shipper Program, an aircraft operator or foreign carrier must submit credentials to the Transportation Security Administration for screening. Europe has a similar program.
- **Port security** – The Transportation Safety Authority has identified crucial issues related to port closures and reopenings in the event of a terrorist attack on a port. The US Coast Guard also runs a maritime-domain awareness program, which tracks vessels and assesses ships' potential for terrorist activities. Current technology lets the Coast Guard follow vessels up to 2,000 nautical miles away from US shores. Experts also use some of these technologies to secure remote oil and gas pipelines, where disruptions could create serious economic and environmental problems.
- **Trucking security** – The trucking industry poses special security issues. Unlike airplanes, rail cars and ships, trucks work in an open environment with unique security concerns. To heighten awareness, the American Trucking Association created a security council and makes annual awards to firms that develop and implement security and emergency preparedness programs. Industry innovations include broader use of bonded, or sealed, freight shipments; increased cooperation with government agencies; and coordination among competing trucking and freight companies. The industry has expanded its use of wireless tracking, including satellite and cellular communications and radio frequency identification, which allow real-time tracing of equipment and shipments.

Threats from the Environment

Mother Nature poses her own massive threats to supply chain security. Rising sea levels will affect ports in particular. One 2007 report found that sea levels could rise by up to 23 inches [58 cm] over the next 100 years, potentially causing coastal flooding that would affect up to 150 million people worldwide. Climate change also could shift the way people grow, procure, manufacture and transport materials. Since climate change affects so many aspects of business, companies should examine their sourcing programs for exposure to disruptions affecting commodity suppliers and other factors that are essential to a firm's long-term business planning.

About the Author

Andrew R. Thomas is Assistant Professor of Marketing and International Business at the University of Akron, Ohio.