pharmaceutical
COMPLIANCE MONITOR

JUNE 17, 2015 WWW.PHARMACOMPLIANCEMONITOR.COM

Chained and Locked–Addressing Pharma Supply Chain Security Challenges

John Lawrence | Pinkerton

When it comes to assessing and addressing security concerns and vulnerabilities in the supply chain, the pharmaceutical industry faces a multitude of challenges. As both the industry and the individual companies within it continue to grow—with a corresponding increase in the size and complexity of individual supply chains—those challenges are only becoming more urgent.

With so many different touch points that go into manufacturing and producing pharmaceuticals, and with more steps and more players involved in the supply chain, there are simply more opportunities for something to go wrong. For any given drug, manufacturing/production, packaging and distribution frequently spans continents and countries, complicating the security issues that need to be resolved before that drug arrives in a hospital dispensary, a pharmacy shelf or a consumer's hands. The worst potential exposures and disruptions can endanger the health and well-being of patients and consumers, and potentially place pharmaceutical companies in financial and legal jeopardy. Even a modest disruption in the supply chain could severely hurt your pharmaceutical operations and revenue if you are not prepared to address it.

> "Engaging in routine information gathering and intelligence sharing on all risks and threats is an important and sometimes underutilized piece of the security puzzle."

Top threats in the pharmaceutical industry today include counterfeiting, with knock-off drugs entering the marketplace and posing a risk to public health, brand reputation and company revenue; theft and pilferage at the pharmaceutical manufacturing site, typically from on-site employees; hijackings and diversions, where even a single diverted cargo shipment can pose a large disruption in product as well as substantial company losses; and the improper or inadequate disposal of damaged or substandard products that can potentially wind up back in the marketplace.

Understanding how these threats manifest themselves, appreciating the various points of physical and operational vulnerability in a 21st Century global supply chain, and knowing how to design, implement and maintain a comprehensive and effective supply chain security strategy is essential for pharmaceutical companies who want to secure their supply chain and protect their organization from avoidable exposure.

Maintain your physical security

From a supply chain perspective, establishing a set of robust, mature and auditable security policies and procedures is largely a top-down exercise. Perhaps ironically, however, the most basic protective measures begin on the ground: with the implementation of minimal physical security standards for manufacturing sites and third-party contract manufacturing (including warehousing and distribution).

A multi-layered approach to security is the most effective way to keep your assets secure, with concentric "rings" of protection that begin with a well monitored and protected outer perimeter. Consequently, securing physical locations that present points of vulnerability in those layers should be a priority. Ensure that your fence/wall/perimeter is routinely checked for weak points and potential breaches. Sometimes the perimeter is defined by the geometry of the building itself. Accordingly, access control systems and cameras should be in place to identify who is going in and out. It makes sense to limit points of access and ensure that all points of entrance and egress are manned.

Segregating shipping and receiving (making sure that any raw material coming in is kept apart from finished product going out) should be standard practice, and all areas where product is being stored or transported should be well lit and well monitored at all times. Scrap procedures are also important: product that does not meet quality standards should be thoroughly and professionally destroyed before being removed from the premises. As a general rule, be cautious about using third-party vendors (with potentially poor oversight) to handle that removal/disposal.

Common mistakes regarding physical security frequently involve damaged or inoperative equipment (have procedures in place to ensure that technology/equipment is working

properly) or the uneven application of security principles across facilities: companies should make sure to apply these standards to both proprietary sites and third-party sites/facilities.

A holistic physical security assessment should review both physical and operational risk, considering the impact of threats and vulnerabilities not just on an immediate physical level, but also downstream: if a facility or a shipment is compromised, what is the broader impact of that for the larger organization? It might sound self-evident, but ensuring that the assets that are most vulnerable and most critical to business operations are also the most heavily secured should be standard practice. Products (and the supply chain infrastructure surrounding those products) that are misused more often are obviously more sensitive.

Do your due diligence

Responsible pharmaceutical companies who value robust security should be performing regularly scheduled security audits of all facilities and processes. Audit schedules and strategies can vary—and will necessarily depend on striking a balance between budget/resources, capabilities and specific risk profiles—but are essential to maintaining a vigilant and responsive posture.

Maintaining due diligence toward partners in your supply chain is also essential: audits should encompass all facilities, operations, and third-party partners/contractors—especially in parts of the world where security concerns are more prevalent. Stringent due diligence policies and procedures should be in place to review everything from freight forwarders and trucking companies, to port and logistics personnel and container management professionals. Comprehensive security audits should ensure that all partners and third-party vendors are following proper procedures, including screening and vetting their employees. When possible, consider making these actions a contractual mandate, including stipulations for regular audits, standard background checks, security reviews and possibly drug tests.

Best practices for a secure operation dictate establishing a schedule to regularly audit locations within your supply chain. Most critical facilities should be visited more frequently. Make sure you are regularly auditing every step in your supply chain, asking if there are any steps in the process that is broken or could be improved. The specific timing of audits depends on the organization, the facilities, the procedures and the details of the vulnerability assessment, but a top-down audit should be perform annually at a minimum—with individual components and procedures reviewed on a more frequent basis.

Prioritize information/intelligence gathering

Engaging in routine information gathering and intelligence sharing on all risks and threats is an important and sometimes underutilized piece of the security puzzle—you cannot prepare for and respond to threats if you do not know what and where they are. Do not neglect resources and insights from collaborative/cooperative industry-specific security organizations like the Pharmaceutical Cargo Security Coalition, the National Biopharmaceutical Security Council, and the Pharmaceutical Security Institute.

In addition to staying abreast of the latest threats to their business operations, pharmaceutical executives can best protect themselves by performing a comprehensive risk assessment: identifying threats to the organization and potential vulnerabilities. Threats and vulnerabilities will vary depending on a number of factors, including demographics, geographic location, crime statistics, the nature of the product or products, and the design of physical facilities and operational architecture. The threat of cargo theft and diversions, for example, is heavily dependent on what part of the world you are in: it is much less of a concern in the U.S. than in countries like Mexico and Brazil, where cargo theft is on the rise.

It is not about just gathering the intelligence, but sharing it throughout your organization and the industry—and about staying ahead of threats whenever possible. From potential natural disasters, to work stoppages motivated by labor difficulties or region-specific political unrest, anticipating significant threats that could threaten to halt or disrupt your operations can literally be a million-dollar difference maker.

To consistently and effectively address the most worrisome threats for your firm, you have to map and understand your entire supply chain—in great detail. This can be an enormous undertaking. If there are scores of different suppliers feeding into a manufacturing site, for example, due diligence obligations can expand exponentially. Subcontracts and delegating oversight can lead to additional complications.

A secure future

For pharmaceutical companies, developing an airtight supply chain management plan needs to be a top priority. Make sure your physical locations are secure, audit your operations to ensure procedures are working and being followed, and keep yourself aware of any looming threats that may risk the disruption of your business.

The good news is that pharmaceutical companies generally understand the importance of protecting their supply chain, and the industry's aggressive response to weeding out counterfeit product that finds its way into the marketplace is evidence of a willingness to deliver a strong and coordinated response. The best strategy, however, is not to respond, but to prevent: to take the basic proactive supply chain security measures that ensure that you are not opening up your organization to unnecessary and potentially damaging risks.

John Lawrence is vice president of Supply Chain & South America for Pinkerton, the global, historic risk management agency. He has extensive experience in managing outsourced security and enterprise risk management programs for U.S.-based multi-national corporations. For more information, visit pinkerton.com.