Complex Chain, Smart Security: How to Protect the Global Pharmaceutical Supply Chain

Your security strategy isn't simple anymore, but that doesn't mean it can't be smart. As the industry has grown and changed, the pharmaceutical supply chain has become more global, introducing new vulnerabilities at each and every stage.

Now is the time to craft a smart strategy you and your company can rely on.

These potential security breaches allow a variety of dangers to potentially leak in, compromising product integrity and threatening public health and safety. Raw materials, active and inactive ingredients, packaging and products face threats both upstream and down, from global sourcing and manufacturing all the way through distribution to dispensing.

Your most pressing challenge is to locate these potential cracks in your supply chain, and design and execute a sound strategy that can help prevent damaging incidents rather than simply reacting to them. As industry leaders responsible for ensuring public health and safety, as well as protecting brand reputation, security directors must rise to the challenge of safeguarding the

© 2015 Tyco. All rights reserved. Tyco is a registered mark. Unauthorized use is strictly prohibited. License information available at www.tycois.com.

supply chain from start to finish. To do this, you must act as advocates for safety measures and product integrity within the pharmaceutical industry, helping to integrate security and operations for optimum efficiency.

This is no easy task, as you well know. But it is achievable through the creation of a proactive security strategy and the implementation of integrated solutions and technologies. As you become increasingly responsible for total corporate risk, now is the time to craft a smart strategy you and your company can rely on.

Know Your Vulnerabilities

Threats come in all shapes and sizes. Two of the primary risks your supply chain faces are adulteration and counterfeiting. Adulteration can be a tricky threat to manage because the motivations of perpetrators can differ widely. Terrorists or disgruntled employees commit a crime for the express purpose of causing harm, presenting a serious threat to public safety and brand integrity. On the other hand, criminals who commit economically motivated adulteration (EMA) want to go undetected, and their actions may or may not cause public harm. However, as the quality of adulterated products is clearly compromised, brand integrity remains at risk.

// The Major Threats

Adulteration: Intentional contamination during the manufacturing process or substitution of ingredients for economic gain.

Counterfeiting: Fraudulent materials, ingredients or products entering the supply chain or deliberate mislabeling of products with respect to identity or source or both.

Diversion: Diverting discounted products intended for one market for resale in another, unauthorized market.

Cargo theft: Theft of products at any stage in the supply chain, including warehouses, containers, truck trailers and couriers.

© 2015 Tyco. All rights reserved. Tyco is a registered mark. Unauthorized use is strictly prohibited. License information available at www.tycois.com.

Ensuring the safety of your source ingredients is a massive challenge with a global supply chain.

Counterfeit raw materials and ingredients entering the supply chain are also an immense risk.[1] For example, in 2006, toxic fake glycerin entered a cough-syrup supply chain through brokers in Panama. The same substitution has been implicated in at least eight mass poisonings around the world in the past two decades.[2] Because pharmaceutical companies source materials and ingredients from many global locations, ensuring the safety of those materials and ingredients is a massive challenge.

As pharmaceuticals advance through the supply chain, the threats continue. Counterfeit ingredients and products can enter the supply chain at various points of vulnerability, for example, through untrustworthy vendors or unsecured storage areas in countries with lax regulations.

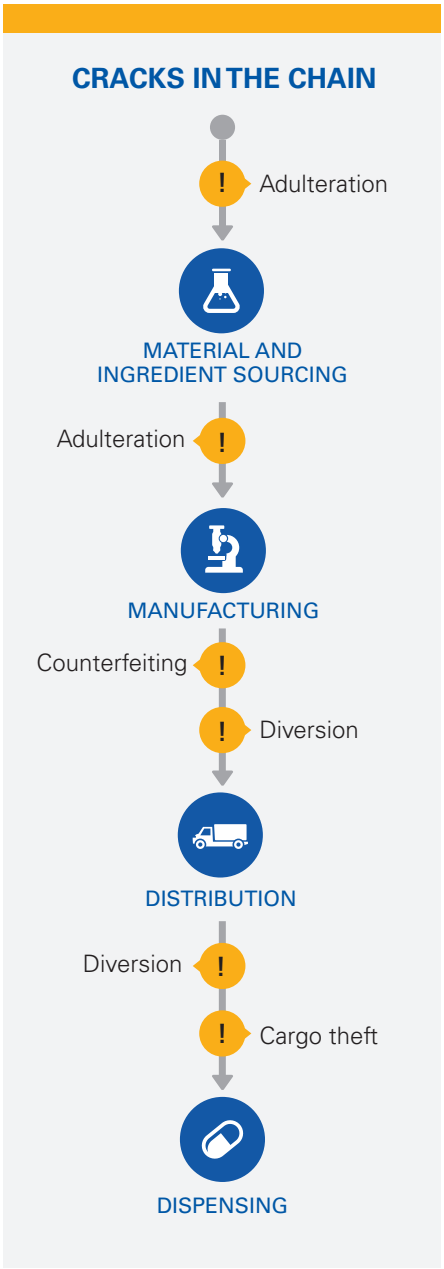
In addition to fake drugs that include no active ingredient, there is also the threat of counterfeiters relabeling real drugs to resemble a higher strength. In fact, the theft of labels, packaging and security devices is also a pressing concern for pharmaceutical manufacturers because counterfeiters often opt to steal the packaging they need rather than create a fake copy.

Although the perpetrators of diversion and cargo theft may not intend to cause public harm, their actions could result in serious hazards by breaking the cold chain of temperature-sensitive products. Additionally, the financial impact of both diversion and cargo theft can be devastating.

A harrowing example of the consequences of counterfeiting came in 2012, when it was discovered that some vials of the cancer medicine Avastin contained no active ingredient. The bogus vials apparently originated in Turkey and eventually made their way to the United States by way of Britain through the help of a Canadian pharmacy.[3] The Avastin scandal is a consequential example of the challenges facing a complex, global supply chain.

© 2015 Tyco. All rights reserved. Tyco is a registered mark. Unauthorized use is strictly prohibited. License information available at www.tycois.com.

FIGURE 1



Threats can occur at any time in the supply chain process.

Understand the Price

First and foremost, securing the global supply chain protects public health and safety. Adulteration and counterfeiting can result in adverse patient reactions up to and including death. In 2007 and 2008, a contaminated blood thinner, heparin, was linked to the deaths of 149 people in the United States.[4] Vulnerabilities in the heparin supply chain precipitated more than just scandal: It was a tragedy.

Preventing another life-threatening situation is certainly top of mind, but it takes daily vigilance and proactive strategies to ensure public health and safety remain a foremost priority, especially as companies tighten budgetary constraints. In addition to breaking customers' trust, failing to protect public health and safety comes with the economic impact of legal costs for damage to health or life. And that responsibility is in your hands.

The financial impact of a security breach can be multifaceted. Along with legal costs, failure to ensure public health and safety can result in product category losses up to forced exit. In addition, not meeting regulatory demands can culminate in Food and Drug Administration (FDA) fines, and diversion and cargo theft can lead to significant financial losses.

The full financial impact of cargo theft can amount to more than just the value of the units stolen. Because pharmaceuticals are still tracked only at the lot level, stolen or otherwise compromised units from one container could potentially trigger a recall of all units in that lot, significantly damaging the bottom line.

On top of all these costs, the impact on pharmaceutical companies may be the largest consequence of all. When brand reputation suffers, the full economic impact can be exponential. Repairing the brand takes time and money, and a full recovery is never guaranteed when customer trust is broken.

© 2015 Tyco. All rights reserved. Tyco is a registered mark. Unauthorized use is strictly prohibited. License information available at www.tycois.com.

When brand reputation suffers, the full economic impact can be exponential.

Four Steps to Crafting a Smart Security Plan

Although the threats to the pharmaceutical supply chain are numerous and the consequences of not securing the chain are devastating, you can mitigate even the most aggressive risks by implementing a proactive strategy through the power of the four A's: Assess, Access, Alert and Audit.

1. Assess Vulnerabilities

The first step in designing a proactive security strategy is to assess vulnerabilities throughout the global supply chain. Remember the variety of threats facing the supply chain at each point (see Figure 1), and consider the specific points of vulnerability from adulteration, counterfeiting, diversion and cargo theft.

Take care to ensure compliance with corporate standards and regulatory requirements throughout your enterprise. Each country you operate in has its own specific regulations, but all systems must meet your corporate standards as well.

2. Control Access

Once you've identified the potential areas of risk in your system, put measures in place to allow only authorized staff access to critical control points. You can prevent unauthorized access to these sensitive areas through integrated video, access control and radio-frequency identification (RFID) tags.

Video surveillance integrated with access control is a powerful solution that works to prevent incidents in addition to recording security breaches when they happen, so you can learn more about specific vulnerabilities and work to address them.

3. Alert Authorities

Once all critical control points are outfitted with the proper surveillance, you'll be prepared to monitor those points and alert the appropriate authorities in the event of intentional or unintentional adulteration or other threats to public health and safety. Remember that detection and rapid response are your sharpest tools to protecting your global supply chain.

© 2015 Tyco. All rights reserved. Tyco is a registered mark. Unauthorized use is strictly prohibited. License information available at www.tycois.com.

Detection and rapid response are your sharpest tools to protecting your global supply chain.

For instance, Physical Security Information Management (PSIM) solutions can automatically link disparate monitoring devices (video, access control, sensors, etc.) to create a complete picture of any security breach or potential breach, allowing you to react quickly. PSIM solutions can also apply corporate policy and regulatory requirements to enforce consistent standards across the global enterprise.

4. Audit Procedures

Finally, to maintain the integrity of your security strategy, regularly audit procedures to ensure operational and regulatory compliance and to provide documentation of compliance to the FDA, Drug Enforcement Agency (DEA) or other regulatory agencies. Make sure to document access to sensitive areas and archive all access records in case of a security breach.

Regular audits promote corporate compliance across the global enterprise, ensuring the longevity and effectiveness of all operational and regulatory best practices. New technological solutions make this essential practice easier and more effective. For example, cloud-based services enable remote video audits so you can keep tabs on every point of the global supply chain no matter where you are. Plus, random video audits are more effective than the periodic check-ins employees expect and prepare for.

© 2015 Tyco. All rights reserved. Tyco is a registered mark. Unauthorized use is strictly prohibited. License information available at www.tycois.com.

Security measures can be operationalized across multiple disciplines.

Begin with Integration

The key to implementing a successful security strategy is to integrate security measures into daily operations. As budgetary constraints tighten, it's important to demonstrate that security measures can be operationalized for optimum value across multiple disciplines.

Video surveillance is a good example of a security technology with multidisciplinary benefits. While it is often dismissed as a tool used solely for security purposes, it can monitor operational compliance as well. Instead of letting the power of video surveillance go to waste by simply monitoring a locked door in an empty corner of a facility, take advantage of the opportunity to track employee movements to maximize efficiency and promote quality and safety procedures.

Integrating security and operational practices is critically important when dealing with a global supply chain because the FDA, DEA and U.S. Customs rely on integrated operational procedures to ensure a consistent standard they can trust. Gaining the trust of regulators through proven consistency and compliance with best practices further ensures efficiency across the global enterprise.

By integrating security with operations and thoroughly documenting every step, you'll be able to present regulators with the information they need to trust the safety and integrity of your raw materials, ingredients and pharmaceutical products. Your customers, too, can rest assured in the trust and safety of your products when you protect your brand's reputation.

As your duties become more complex and the threats to the global supply chain become more pervasive, it's important that you understand how to implement the necessary measures to protect not only the product but also the patients using it.

© 2015 Tyco. All rights reserved. Tyco is a registered mark. Unauthorized use is strictly prohibited. License information available at www.tycois.com.

Support You Can Count On

Tyco Integrated Security has the global expertise and integrated technologies to help you protect product integrity and security across the global supply chain. TycoIS understands the complexities of international security regulations and can help you maintain corporate compliance across the global enterprise. Most of all, TycoIS shares your passion for ensuring public health and safety.

TycoIS can help you stay up to date with the changing pharmaceutical security landscape, so you can keep up with new regulatory requirements. TycoIS also provides the cutting-edge integrated technological solutions you need to implement the four A's, in order to continue protecting the integrity and security of your products, ensuring public health and safety, and upholding your brand's reputation.

// Learn more about the TycoIS pharmaceutical supply chain solutions at TycoIS.com or download the brochure.

Sources:

[1]Carolyn Becker, Esq., "Overview of How FDASIA Became Law," 2014 PDA/FDA Pharmaceutical Supply Chain Conference, http://www.pda.org/docs/default-source/attendee-presentations/north-america/2014/2014-pda-fda-pharmaceutical-supply-chain-conference/carolyn-becker.pdf?sfvrsn=14 (accessed February 17, 2015).

[2]Walt Bagdanich and Jake Hooker, "From China to Panama, a Trail of Poisoned Medicine," *The New York Times*, May 6, 2007, http://www.nytimes.com/2007/05/06/world/americas/06poison.html?pagewanted=all&_r=0 (accessed February 17, 2015).

[3]Gillian Blease,"Fake Pharmaceuticals: Bad Medicine," *The Economist*, October 13, 2012, http://www.economist.com/node/21564546 (accessed February 17, 2015).

[4]Ibid.

© 2015 Tyco. All rights reserved. Tyco is a registered mark. Unauthorized use is strictly prohibited. License information available at www.tycois.com.