SC Security & Pharma:

A Disconnect?

There are many security issues within the pharmaceutical industry–counterfeit drugs, theft, loss, pilferage, delays in shipment, contamination, patent infringement and more. What to do to solve some of these problems is the obvious question and challenge. However, while it appears that attacking just one fundamental vulnerability in the industry - the control of the product from the origin through its shipment to destination- would result in many advantages, it simply is not done, or it is done in a manner sufficient to accomplish its purpose, observe **Dr Jim Giermanski** and **Ian Schmehl***

Controlling the supply chain not only protects the public, but also improves the bottom line. This analysis will focus on solving some, if not most, of the vulnerabilities associated with control and movement of pharmaceutical products within the supply chain, specifically: verification of container contents at origin, container temperature and internal environmental controls, access, tampering, movement monitoring, and authorized access at destination. Control of this type treats many risks from corruption to theft. Take for example, the role and negative impact on the industry and the public of counterfeit drugs.

A Problem: Counterfeiting

With the advent of technology our lives have been made easier and our borders extended through a globalized economy. Because of this global economy, it has become easier to introduce illegitimate pharmaceutical products. A harsh truth that we as a society must now face is that the pill prescribed by our doctors may no longer be what one thinks it is and thus not do what was hoped it would. Counterfeit pharmaceuticals are a growing threat to our society. The rise of illegal medications is not only alarming, but possibly deadly. This is a problem not unique to developing countries. It is well entrenched here in the United States.

On June 15th of this year, "Fake Viagra" was found in the legitimate supply chain in Australia. This level of compromise to the supply chain is cause for alarm. To combat a problem the key is to first understand it – counterfeit pharmaceuticals is no different. "The U.S.-based Center for Medicine in the Public Interest predicts that counterfeit drug sales will reach $75 billion globally in 2010, an increase of more than 90% from 2005." Secretary Tommy Thompson who served under President Bush, and Secretary Donna Shalala who served under President Clinton have both stated that they cannot certify the safety or cost-savings of imported prescription drugs from foreign countries. The World Health Organization says that up to 10% of medicines worldwide are counterfeit—a deadly hazard that could be costing the pharmaceutical industry $46 billion a year.

On May 14 2010, the Miami Herald reported that "The FDA, along with Customs and Border Patrol and the U.S. Postal Service conducted at the Miami International Airport "Operation Safeguard," which had dozens of agents pouring through piles of packages filled with illegal pharmaceutical drugs, dietary supplements and home remedies mailed from foreign countries." Statistics and increased government enforcement underscore the need to understand better

Dr. Jim Giermanski is Chairman, Powers Global Holdings Inc and Ian Schmehl is Director, Labor Relations, AT&T

counterfeit pharmaceutical operations, to identify solutions to protect citizens who want a prescription to address their needs, not a more serious problem that may have to be treated.

A Solution: Controlling the Global Supply Chain First

While some claim that the unfettered access to pharmaceuticals through the internet is the problem, perhaps it really isn't. Placing blame on the internet since the internet as a medium is efficient, effective, and global, may be off the mark. While it is true that social media have come to play a more prevalent role in access to illegitimate and often dangerous pharmaceuticals, the "Tweet" may not be the core issue. A routine tweet from a user can be troublesome for the industry. For instance, Phil Taylor of Securing Pharma wrote "A Canadian website classified as a rogue online pharmacy by LegitScript is using Twitter to advertise medicines, indicating the battle against the illegal medicines trade must also be fought on social media platforms." True, but without controlling pharmaceutical trade and global access to unsecured drugs and medication, the internet would have a lesser role to play. The ability to monitor internet groups, sites, and communications is immensely difficult and trying to weigh the policing of the internet with the safety of the citizens is difficult if not impossible. There are no borders to this problem; there are no limits to its reach. In light of this, it seems the solution must begin and be maintained by supply chain security methods. There are supply chain solutions, from the simple security seal to the sophisticated smart container. So what exactly is needed? There are today "off the shelf" smart container systems that can provide global control and maintain the integrity of the international and domestic pharmaceutical supply chain.

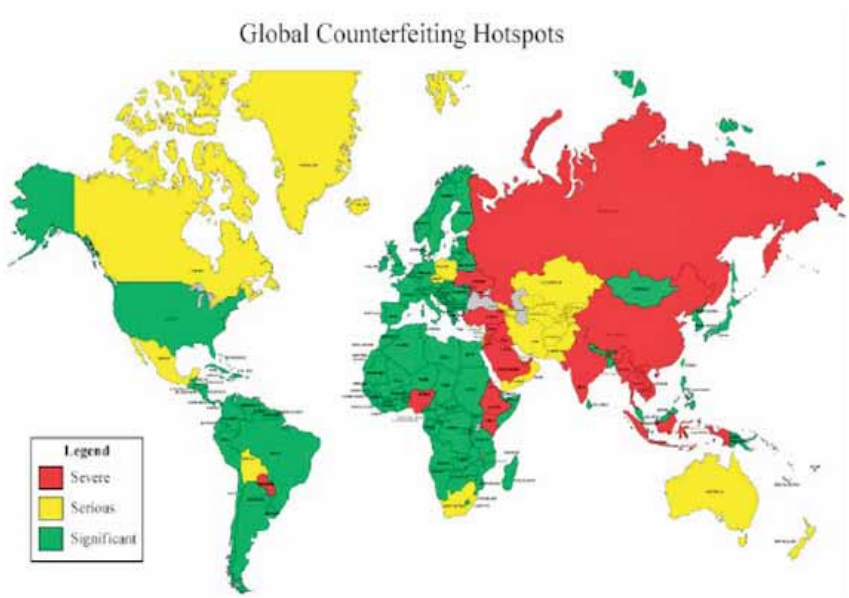
What is needed is often unique to the producer and pharmaceutical cargo. If you are a pharmaceutical company like Pfizer, Inc., you may need to continuously monitor the container's internal environment like temperature, and for its high-value cargo like Viagra, security against theft. Smart containers can also detect surreptitious

access for the purpose of stealing legitimate drugs or adding illegal drugs to the legitimate cargo of a reputable pharmaceutical company. In general, while different shippers, carriers, and consignees have different needs, the basic features of smart containers include the carrying of logistics and manifest data, container movement and location monitoring through historical and/or real-time reporting; detection and reporting of unauthorized access or breach through any portion of the container; internal environment monitoring and the reporting of temperature, excessive vibrations, and even the presence of foreign substances.

The Instruments of Control: Smart Containers

Smart containers exist today and can mitigate and eliminate threats to the integrity of a pharmaceutical shipment. These solutions begin at the container's stuffing, and remain through distribution to destination where the unloading is controlled. There are a number of different types of supply chain security measures that are implemented to combat counterfeiting, tampering and theft. Their sophistication ranges from simple reporting of location when it is interrogated by a land-based transceiver, typical of land-based, historical RFID (radio frequency identification) technologies; to tracking and tracing features provided by satellite and cellular technologies; to actual real-time detection and reporting of a container's internal environment and integrity; to the ultimate chain-of-custody system controlling and monitoring from origin to destination. Some containers are simply more intelligent than others because of how they are equipped and programmed. Each type provides a different benefit for varying users. For example, if you are a national retailer, you might want to know only the location of your container because of its potential role in inventory availability connected to your promotional events in different regional markets. Governments, however, may care only about the location of their sensitive or hazardous cargo. Yet other shippers want to ensure that the contents of their containers are not contaminated or deviate from a prescribed route of travel, called geo-fencing. For instance, a container programmed with geo-fencing detects a variance between where it should be and where it is, suggesting a hijacking or being sent to the wrong consignee or the wrong location. Each benefit is programmed based on the specific needs of the shipper, carrier, or consignee.

Simple security seals can safeguard access, and deter theft and provide product safety. Their sophistication ranges from simple barrier seals to electronic seals which report



location only when they are interrogated by an RFID (radio frequency identification) land-based transceiver; to tracking and tracing features provided by satellite and cellular technologies; to actual real-time detection and reporting of a container's internal environment and integrity; to a chain-of-custody system from origin to destination. Container security providers offer different levels of sophistication and detail. Firms like TrakLok, LoJack, FreightWatch and GateKeeper offer electronic container security devices today. Barrier and electronic seals are also offered by Sealock. There are also advances in container design and construction. For instance, Cakeboxx offers a shipping container without doors. In fact, its uniqueness and applicability of all types of cargo will be highlighted by the World Customs Organization in its October 2010 edition of WCO News.

The present smartest container has a sophisticated, comprehensive chain-of-custody system that begins at the stuffing (loading) of the container at origin and maintains, monitors, and reports its integrity to the end of the global supply chain path at destination. Its process includes the human element in the supply chain. No system is 100% effective, and one cannot depend on technology alone. Because technology often overshadows the role of humans in security systems, container systems have to include the identification of the party responsible and personally accountable for final inspection of the cargo prior to the container's sealing, dispatch and subsequent international movement to destination. Someone must necessarily be identified and responsible for confirming the cargo on the bill of lading or booking sheet, for activating the smart container system, and for locking the doors. This responsible party must be vetted with respect to integrity and competence. Equally, there must be a counterpart at destination. Both parties are electronically connected by a unique identifier to the smart container to complete the system. This is how it can work. An electronic activation key or equivalent that contains bill of lading and booking information, or information needed by Customs authorities, and other data such as the identity of the supervising and arming agent at origin and the final agent deactivating the system at destination is inserted into the container security hardware. Therefore at activation, the accountable party becomes an integral element in the smart container security system, and once the container is activated by using an electronic key protocol, these data can be read at almost any time during the container's voyage by satellite communication. The activation also allows the smart container to notify appropriate parties of an unauthorized breach or to report the condition of the container or, depending on the sensors used, to report the type of the cargo within the container and even to report its own hijacking.

When a smart container is opened at destination by an equally accountable person and cargo is missing, and there were no breaches detected, recorded and reported, the accountable person at origin can face either disciplinary, or worse, criminal action by appropriate authorities. A worldwide control centers offer the capacity to serve as a third-party electronic record of the transaction recorded automatically in its servers. Thus, smartest container offers an electronic receipt of delivery, accomplished by the opening of the container by a person at destination approved and authorized to open the container, which is provided by another specialized electronic key protocol usable only with and by an authorized individual at the point of destination. In summary, a smart container provides the following benefits:

- Electronically identifies the authorized personnel stuffing and securing the container, and accepts and report information like container/trailer number, booking data;
- Carries and reports logistics data, including container number;
- Detects and reports a breach in any part of the container in real-time or close to real-time;
- Tracks the container through the supply chain;
- Identifies authorized personnel unsealing container; and
- Accommodates disparate logistics programs in communicating critical data.

So far, only European Datacomm (EDC), and GlobalTrak in the United States can today provide these smart containers.

The Costs of Smart: None

One presumes that the pharmaceutical industry already knows the costs of counterfeit products, theft, contamination, loss, fraud, and supply chain inefficiencies. And one way or the other, the private sector really pays for all of this. Even our government, in trying to encourage smart container usage recognized that there would be a push back from the private sector. Knowing this, Customs and

Border Protection (CBP) commissioned the University of Virginia to determine the cost/benefit outcome to taking security measures. Published in a 2007 cost/benefit survey report, CBP reported the following with respect to benefits of simply participating in it Customs Trade Partnership Against Terrorism (C-TPAT) program:

1. Fewer examinations (34.4% decrease)
2. Better supply chain visibility (29.4% better)
3. Predicting lead-time (24.3% better)
4. Tracking orders (22.2% better)
5. Disruptions in supply chain (28.9% fewer)

Unfortunately, it seems that the return on investment (ROI) is either not known to, appreciated by, or significant enough to the user to employ smart containers. Or the user is simply focusing on the costs involved in using smart container technology, not weighing the bottom-line benefits of a visible supply chain and the automatic positive impact on counterfeiting activities and other supply-chain related costs. Yet, it is recognized that, at a minimum. there will be a positive financial impact and savings through Customs expedited treatment of containers using smart container containers as defined in the SAFE Port Act. The benefits of expedited shipments, alone, vary from $600 to $700 per container per move (Bearing Point Study, 2003); and $1150 per move (AT Kearney Report, 2005). Therefore, if a smart container costs you an additional $100 from origin to destination, and you save $1000 on the expedited treatment, what was the cost? Costs are associated with the loss or delay of cargo; diversions; increased insurance premiums; supply chain disruptions; increased labor to reship or replace the cargo; business downtime; loss or delay in medication release; or the loss of sales. Benefits include minimizing financial risks, reduced inventory carrying costs, protection against counterfeiting; reduced or eliminate diversion costs, reduced out of stock, and reduced insurance costs.

Conclusion

There is no argument that the loss of a 40' container of Viagra worth millions, or its counterfeiting, or its contamination, or its delay, or its pilferage is significant. There also is no argument that smart containers, especially those that provide the chain-of-custody process are available to solve these problems. Finally, there is no argument that additional revenue results from using smart containers. It simply appears that the pharmaceutical industry's executive and security leadership has failed to respond to fundamental supply chain vulnerabilities. It also suggests that the insurance industry is willing to pay claims even though the shipper may be at fault for not taking appropriate available action to secure the shipment–but that's another story!

Stanford Study

A Stanford University recent study revealed that quantifiable benefits of security controls and technology included:

- Improved Product safety – 38% reduction in theft/loss/pilferage, 37% reduction in tampering;
- Improved Inventory management – 14% reduction in excess inventory, 12% increase in reported on-time delivery;
- Improved Supply chain visibility – 50% increase in access to supply chain data, 30% increase in timeliness of shipping information;
- Improved Product handling – 43% increase in automated handling of goods;
- Process improvements – 30% percent reduction in process deviations;
- More efficient Customs Clearance – 49% reduction in cargo delays;
- Speed Improvements – 29 % reduction in transit times;
- More Resilience - 30% improved response time; and
- Higher Customer Satisfaction – 26% reduction in customer attrition and 20% increase in new customers.

Other sources offer different, but compelling, benefits to using smart container technology to include the U.S. Congressional Budget Office, in March 2006. In a 2006 A.T. Kearney survey report, respondents stated that "…they need real-time data for accurate visibility into their supply chains." Since accurate data do not exist within the current logistics industry, smart boxes can provide that missing data deemed important to shippers. The report further revealed that the U.S. Department of Defense is now utilizing smart containers even though they are not the smartest containers. These smart boxes "…reduced overall losses (military supplies) to less than 8 percent." There is a favorable bottom line to using smart boxes based on speed alone. The A.T. Kearney, Bearing Point, Stanford, and Congressional Budget office all, in one way or another acknowledged that control and speed through the supply chain, and especially through ports, pay off.

Sources

Staff Reporter, Fake Viagra found in Australia's legitimate supply chain, June 21, 2010, http:www.SecuringPharma.com.

Counterfeiting Facts and Stats, Protection from Brand Infection, CMO Council, April 28, 2009, http://www.cmocouncil.org/programs/current/protection/protection_counterfeit_stats.asap, May 26, 2009

Frederick Balfour, Ami Barrett, Diane Brady, Kerry Capell, Paul Magnusson, Carol Matlack, Dexter Roberts, William C. Symonds, and Johnathan Wheatley, Fakes!, Business Week, February 2005. http://www.businessweek.com/magazine/content/05_06/b3919001_mz001.htm, May 26, 2009.

Reuters, Counterfeit drugs on the rise, pose global threat: WHO, May 2010, http//www.reuters.com/articleidUSTRE6416G120100519.

Phil Taylor, Rogue pharmacies turning to Twitter to peddle drugs, May 6, 2010, http://www.SecuringPharma.com

For an expanded treatment of smart containers, see Dr. Jim Giermanski, Smart containers: their use, their payback, WCO News, October 2009, pp. 23-25; and for an expanded technical treatment see Dr. Jim Giermanski, Container Security: Is it working?, Logistics Management, October 2009.

Robert W. Kelly, JD, Containing the Threat: Protecting the Global Supply Chain Through Enhanced Cargo Container Secuity, The Refore Institute, October 3, 2007, pp.8-9.

Abdoulaye Diop, Ph.D., David Hartman, Ph.D., Customs-Trade Partnership Against Terrorism Cost/Benefit Survey Report of Results, Weldon Cooper Center for Public Service, University of Virginia, August, 2007, p. 47.

Barchi Peleg-Gillae, Gauri Bhat, and Lesley Sept, Innovators in Supply Chain Security The Manufacturing Institute, Stanford University, July 2006, p. 4.

Smart Boxes, A.T. Kearney, July 28, 2006, p. 1.

Smart Boxes, A.T. Kearney, p. 2.