Rx-360 Supply Chain Security White Paper:

A Comprehensive Supply Chain Security Management System

Version 2.0

Original Authors	Revision Authors
Ron Guido (J&J)	Reggie Jackson (Pfizer)
Rod Stull (AstraZeneca)	Hazel Aranha (Sartorius)
Jyrki Syvaeri (Boehringer Ingelheim)	Elizabeth Robinette (Eli Lilly & Co.)
Anthony Zook (Merck)	
Jeremy Baumann (Takeda)	
Linda Mikulan Maxfield (Baxter)	
Dave Osbourne (Genentech)	
Tim Valko (Amgen)	
Matt Yedwabnick (Amgen)	

Created: 16 April 2012
Revised: 7 November 2019

Executive Summary

Protecting patients is a key core value of the pharmaceutical industry and is fundamental to our business. Supply Chain Security (SCS) includes the prevention, detection, and response to intentional adulteration, theft, counterfeit, and diversion that threaten patient safety. These threats have been on the rise for over a decade as the supply chain has become increasingly complex.

To combat this growing concern in the global supply chain, an integrated approach to managing security risk across the supply chain is needed. Through the open collaboration of Rx- 360 companies, the SCS Initiative seeks to improve the practices of security across the industry and its supply chain. The objective of this white paper is to share the concept of a comprehensive management system that can provide a common perspective and set the foundation of a maturity model that will drive the measurable and sustainable improvement of these practices.

Introduction

The industry and its regulators, the U.S. Food and Drug Administration (FDA), European Medicines Agency (EMA), and other regulatory bodies, are concerned that the drug supply chain has grown extremely vulnerable to a variety of illegal activities that could have serious public health implications. Many regulatory bodies have enacted different legislation to combat this, such as the Drug Supply Chain Security Act (DSCSA) in the US and the Falsified Medicines Directive (FMD) in the EU. Given this, Rx-360 member companies are paying significant attention to the supply chain security of their operations and are collaborating to improve SCS in the industry to help support patient safety.

SCS can be defined as the prevention, detection, and response to:

(1) intentional adulteration,
(2) theft,
(3) counterfeiting, and
(4) diversion of product/packaging components and/or finished goods.

These categories can overlap, such as when stolen pharmaceutical products are altered and reintroduced into the market or when counterfeits are sold as diverted products. These threats must be countered with an integrated approach and refined through a process of continuous improvement. These threats are: (see Appendix 3).

(1) Intentional adulteration incidents that occur prior to or post manufacturing. An example of adulteration prior to manufacturing is when unscrupulous suppliers of raw materials or packaging components deliberately dilute or substitute ingredients. In doing so, they compromise the product's integrity and safety. Incidents can go unnoticed without robust supplier screening and auditing practices in place. The growing threat to patient safety of intentional adulteration is highlighted by examples of adulterated Heparin, infant formula, pet food, and cough syrup. Post manufacturing adulteration involves tampering with the drug product, e.g., opioids and placing other material in the same package.

(2) Theft of products or components can occur at any stage of the supply chain. Within the category of theft, the theft of finished drug products poses the most serious risk to patient safety given the potential for those stolen products or packages to re-enter the legitimate supply chain with compromised quality. The importance of countering the threat of theft was high-lighted by the FDA's recognition (in a letter to stakeholders) that cargo theft and diversion are a serious threat to patients.

(3) A counterfeit medicine is one, that is deliberately and fraudulently mislabeled with respect to identity and/or source. E-commerce has provided a gateway for these illegitimate products, which falsely associate themselves with reputable brands to give themselves credibility. This has led to a large rise in illegal online pharmacies as well as online marketplaces distributing them. (Davies. W. 2018) Counterfeiting drugs is very profitable for criminals. In many countries, the risk of being caught and the severity of the punishment for selling fake medicines is relatively low. This makes the sale of counterfeit drugs more lucrative and less risky as compared with selling illegal drugs. According to a report published Feb 25, 2019 by Anaheim Lighthouse the arrival of large amounts of "counterfeit prescription drugs containing fentanyl" is causing an explosive growth in overdose deaths in the United States. Counterfeiting occurs worldwide and is more prevalent in developing countries, but the true extent of counterfeiting is unknown.

(4) Diversion is the criminal rerouting and resale of pharmaceuticals intended for use in a different location. This can be internal diversion locally within a market or external diversion between global markets. The dangers of diverted product are often not clear to the public. Although some instances of diversion simply involve the transfer of legitimate, safe goods from one consumer market to another, patients cannot be assured that diverted products are of good quality. Sources of diverted product may include stolen products that were donated to a relief organization or counterfeit drugs, as was the case with the 2012 Avastin event (see Appendix 1). Diversion is one means by which counterfeits are inserted into the legitimate supply chain.

Additionally, diversion can compromise a product's cold chain, in which the product requires strict storage temperature and humidity controls in order to remain effective and safe.

The 2012 case of counterfeit Avastin demonstrates how the threats of diversion and counterfeit can be connected and must be addressed through an integrated approach. The case also highlights that more work is needed from the industry, its regulators, and the medical community to help ensure the safety of the supply chain.

As has been stated by regulatory agencies: "What we're concerned about is putting in place systems to prevent greater and more widespread problems in the future."

The Consequences of Supply Chain Security Breaches

Patient safety is unequivocally the primary driver for SCS. Individual companies are legally and ethically obligated to help secure their supply chains in order to minimize risks to patient safety. In addition to legal and ethical requirements, improving SCS will help companies avoid the costs of breaches in security. While some of these losses are clear, others are relatively invisible. Types of loss include:

(1) revenue loss;
(2) recall costs;
(3) litigation costs, and
(4) product approval costs.

Beyond simply the avoidance of losses, it is imperative to recognize that patient safety is a key component of patient trust and therefore a vital business interest to the entire industry.

Revenue losses from SCS breaches include the costs of all lost or stolen inventory, cost of re-manufacturing, the costs of increased insurance, and the loss of sales. Hidden costs for firms due to diversion include the increase of operational costs of inventory due to the shifting demand. In cases of adulteration and counterfeiting, companies lose future revenue from customers dissuaded from buying product(s) from the affected firm. This loss in future sales reflects erosion in the firm's brand equity.

Recalls triggered in response to threats to patient safety often carry significant costs. The goal of a product recall is to prevent stolen, adulterated, diverted, or counterfeit goods from re- entering the supply chain without detection. Business interruption costs may occur as the company forgoes any profit from lost sales during the recall and beyond.

Product approval costs occur where a company suffers setbacks in regulatory approvals as the result of supply chain breaches. Active comparator studies, which compare the efficacy of developmental drugs against competitors with proven effectiveness, are common and critical. The risk of counterfeit or adulterated drugs being included in active comparator

studies cannot be overlooked. In addition to threatening patient health, compromised drugs pose a threat to regulatory approval if clinical trials are based on comparisons to counterfeit products.

The value proposition for a comprehensive SCS program goes beyond the avoidance of these losses. Patient safety is legally, ethically, and economically in the best interests of every company. The entire industry can benefit from increasing patient safety by using an integrated and comprehensive approach to SCS. As criminal elements succeed in compromising safety, independent regulatory bodies across the globe will increasingly institute requirements and punitive measures for negligence, which will increase the complexity and management costs of the supply chains. This will also erode the confidence our patients and the public have in the pharmaceutical industry as good stewards of health. Our industry is in the business of improving the lives of patients through the safety and efficacy of its products and SCS is a key piece of that value proposition.

A Comprehensive Supply Chain Security Management System

Pharmaceutical supply chains are becoming increasingly complex from end-to-end as more raw material suppliers, packaging components suppliers, manufacturers, and logistics providers play a role in the global supply chain. To address this complexity, Rx-360 companies have collaborated on the SCS initiative to improve the practices of security across the industry and its supply chain. This framework consists of key program attributes and elements that describe efforts to prevent, detect, and respond to threats. Rx-360 companies and regulatory agencies are moving to align their management structures to focus on SCS holistically, from raw materials to patients.

Given the threats to SCS, the global pharmaceutical supply chain can be simplified into four key phases from a security standpoint:

(1) Raw Materials,
(2) Production,
(3) Logistics, and
(4) Market.

To align with this view of the supply chain, this framework has described key attributes:

(1) Supply Chain Transparency and Supplier Management,
(2) Packaging Technology and Manufacturing Controls (Internal and External),
(3) Warehouse and Cargo Security, and
(4) Market Monitoring and Product Integrity.

Table 1 illustrates this relationship. Each phase has key attributes, but the approach is integrated: program elements will overlap across phases at the detail level.

Table 1 – Key Program Attributes by SCS Phase

SC	SC Phase	SCS Key Attributes	Examples of Program Elements
Raw Materials Packaging Components	Sourcing	Supply Chain Transparency and Supplier Management	➢ SCS elements are integrated into Supply Agreements, Quality Agreements, Standards, oversight, and selection of suppliers ➢ SCS applies a risk-based approach to supplier management
Internal Mfg. External Mfg.	Production	Packaging Technology and Manufacturing Controls	➢ Packaging technology and security features are managed comprehensively and implemented at internal and third party manufacturing sites ➢ Management System for third party manufacturing and packaging.
Transportation Warehousing	Logistics	Warehouse and Cargo Security	➢ SCS elements are integrated into Service Agreements, Standards, and selection process for LSPs and Distributors ➢ Site and Conveyance security is managed comprehensively using a risk-based approach
Distributor Provider Consumer	Market	Market Monitoring and Product Integrity	➢ Market surveillance, investigation and enforcement, external advocacy, and market education ➢ Product integrity authentication

Sourcing - Supply Chain Transparency and Supplier Management

The supply chain starts with the manufacture of high quality raw materials or products by third party suppliers. Companies should have very effective processes to select only trusted and qualified suppliers. One Quality Standard should be used for internal sites and suppliers, which provides a strong governance structure across the supplier networks. SCS will be additive to existing Quality Systems and will take a risk-based approach such as using raw material risk assessments to characterize raw materials and stratify suppliers based on risk and taking mitigation actions accordingly.

Quality Management Systems should include contracts and/or Quality Agreements with suppliers to communicate standards and expectations. Routine Quality Assurance and Corporate Integrity and Business Continuity audits should be conducted at supplier sites. The processes used to monitor the ongoing safety and integrity of products are risk-based and include the oversight of deviation management, change control, complaint management and escalation, documentation review, and testing.

Industry Collaboration and Supply Chain Transparency

Companies are increasingly relying on collaboration with other supply chain stakeholders to mitigate risks. This is fast becoming an industry norm and an important part of a comprehensive SCS program. Rx360 is such a consortium, which is very active and has a robust Quality Intelligence program. Their supplier management systems include excellent communication between companies and suppliers, including notification of Quality issues and improvement plans. They monitor the external environment for material shortages, profiteering and political issues, which could lead to Quality or Compliance incidents and communicate these risks broadly.

Information and results from inspections are shared between members, which provide more information regarding suppliers' compliance performance. The group has developed excellent relationships with regulatory agencies, such as FDA and EMA, and communicates known issues, creates information bulletins, and shares best practices.

Collaboration among Rx-360 members and regulators will better address risks that affect the entire industry, as seen in the response to the 2011 Japan natural disaster (See Appendix 2). The Rx-360 working group actively shared information, practices, and risk-based approaches to address supply chain impacts from the earthquake, tsunami, and radiation events. The working group then met with the FDA for a comprehensive information exchange.

Production Phase – Packaging Technology and Manufacturing Controls

Packaging authentication and security features are a critical aspect of ensuring product integrity. A comprehensive program includes risk-based use of minimum-security requirements for primary, secondary, and other packaging across regions or the globe, including licensing partners. These features should provide overt, covert, and forensic level authentication as well as tamper features on packaging. Firms are encouraged to pursue qualified backup security technologies as part of a rotation or in response to an incident. Finally, a firm should conduct periodic authentication and security feature assessments.

For product authentication, DSCSA and FMD law now requires companies to serialize their products to prevent counterfeit products from entering the supply chain. Serialization entails imprinting of a serial number (i.e., unique identification information) directly onto the product packaging. The serial number is then officially registered in a secure database as soon as the manufacturer introduces the serialized product into the supply chain. As product hand-offs occur between business entities, the recipient can determine product authenticity by verifying that its serial number was registered by the manufacturer. There are also other verification techniques such as pedigree or track-and-trace, both of which

require serial numbers to be effective. Pedigree involves exchanging product (represented by serial numbers) movement history directly between business entities. Track-and-trace refers to recording of events, such that as the products exchange hands their serial numbers are reported to show transfer of physical possession

When outsourcing manufacturing, firms should have comprehensive supplier quality management programs in place to only work with qualified and trusted contractors. These programs should cover selection, contracts, and risk based oversight with supply chain security processes well integrated. Comprehensive site security programs are also critical for internal and external manufacturing sites as described below.

Logistics Phase - Warehouse and Cargo Security

Having effective site/warehouse security standards and practices in place to protect materials and products at each step of the supply chain (manufacturing, wholesalers, distributors, carriers, repackagers, etc.) is essential. Companies should have processes to ensure the utilization of tiered physical site security standards that include physical, electronic, and procedural components. These risk-based processes include: fencing, guards, electronic entry, intrusion detection, monitors, auditing, personnel procedures and written standards and apply wherever goods are stored in the world.

The conveyance standards and management of transportation enhance cargo security. Safely moving goods prior to and after manufacture is key to preventing theft, diversion, and counterfeits entering and exiting the legitimate supply chain. Companies should use sophisticated processes to ensure they control the movement of all their goods. Conveyance security standards should be established that typically include: shipping and receiving controls, container security features, container inspection, use of seals, personnel background checks and integrity audits, threat awareness, physical site security, driver training, theft prevention, cargo tracking, and documentation controls. When outsourcing any logistics services to a third party, companies should have processes for selection, establishing contractual expectations, and monitoring the performance of their service providers. These are global standards/processes and apply wherever goods move in the world. The prevention of cargo theft must also take a regional approach, as security techniques may not be effective in all regions.

Market Phase - Market Monitoring and Product Integrity

Companies use many processes to continuously monitor the performance and safety of their products globally. The focus is on prevention but processes to detect and respond to counterfeit, stolen, or diverted products should also be in place. These processes are collaborative efforts with regulators, customs, and law enforcement. Complaint and adverse event processes are typically used to identify quality problems associated with legitimate product, however, these same processes are also effective in detecting diverted, counterfeit, stolen, and intentionally adulterated product. Through company security organizations and in collaboration with law enforcement, criminal activity is monitored to identify trends or respond to specific threat intelligence.

Companies should actively integrate SCS into common trade practices via Distributor/Wholesaler Oversight. Companies should work closely with their trading partners in the market to ensure the safe distribution of products to consumers even after transferring possession of their products. Processes should be in place to ensure firms are only selling to trusted and qualified wholesalers. Requirements typically exist to ensure they only purchase directly from the company and apply the same conveyance and site security standards expected internally. Processes exist to monitor wholesaler performance against these standards. This is all designed to protect the integrity of the legitimate supply chain against counterfeit drugs entering and the diversion or theft of legitimate product.

The Comprehensive View of Supply Chain Security

The following framework is meant to be representative of a comprehensive system and it is not to be taken as a literal list of requirements. It is up to a firm to analyze the framework with reference to their specific business conditions to determine which elements become requirements. Firms are strongly encouraged to use a risk based approach to prioritize improvements where needed.

Table 2 - End-to-End view Categorizes Phase Elements as Prevention, Detection, or Response

	Sourcing	Production	Logistics	Market
Prevention	• SCS integration: Supply Agreements, Quality agreements & selection • Supplier risk and security assessments • Material qualification	• SCS integration: Contractor agreements & selection • Contractor risk & security assessments • Anti-counterfeiting Packaging • Waste management and asset disposition rules	• SCS integration: LSP agreements & selection • Risk and security assessments • Conveyance standards • Site security standards • Shipment value limits	• SCS integration: Wholesaler agreements & selection • Supply controls • Direct to pharmacy model • Samples/free goods management • Reverse logistics • Patient education • External advocacy
Detection	• Material inspection & testing • Supplier auditing • Market intelligence	• Serialization • Overt & Covert security features • Surveillance testing • Contractor auditing • Contractor oversight • Licensing and acquisition support	• LSP auditing • Shipment tracking systems • Certified cargo screening program • Threat awareness & training • Return goods policy	• Market intelligence • Complaint handling • Authentication / forensic testing • Sales force, provider, & consumer education • Sales & internet monitoring • Parallel trade monitoring
Response	• Adulteration Incident management • Adulteration investigation/CAPA • Continuous Improvement	• Counterfeit and Theft Incident management • Exit strategies • Continuous Improvement	• Theft Incident management • Regulatory Agency, Law enforcement/customs collaboration • Theft response program • Continuous Improvement	• Counterfeit and Diversion Incident management • Enforcement • Internet education • Counterfeit education • Public affairs policy

Some elements are present in different forms across the supply chain. Examples of multi-phased elements are the different types of risk assessments and the different forms of incident management. Other elements, such as the serialization of products, reside primarily in the area where they are implemented, but are dependent on elements in other phases such as authentication in the market and the return goods policies. Often times an element can be common across multiple types of countermeasures such as the prevention and detection aspect of cargo screening, but are simplified to their primary role in SCS, in this case detection. Exceptions exist, such as with education and awareness, which is specifically called out as a primary method of prevention, detection, and response to SCS, threats.

The Rx-360 SCS initiative has developed additional tools and reference materials designed to improve SCS practices across the industry. One example of this is a maturity model designed to assist companies that have a supply chain security management system in place.

The management system described here will provide a foundation to understand the threats and develop those practices in context. Rx360 SCS initiative is committed to continuing collaboration among companies and with regulatory agencies to help improve patient safety.

Conclusion

Securing our supply chains and preventing counterfeiting, diversion, theft, and intentional adulteration will require collaboration between companies and all supply chain partners, regulators, and law enforcement. Companies should actively engage in industry wide associations and consortia also working on SCS; including Rx-360, Pharmaceutical Safety institute, Pharmaceutical Cargo Safety Coalition, Parenteral Drug Association, and Partnerships for Safe Medicines to name a few.

We believe the industry needs to work together to succeed, as criminals will exploit the weakest links in the supply chain. Finally, this Comprehensive SCS Management System is grounded in the concept of continuous improvement. The criminal elements we are combating will be continually adapting to circumvent our best efforts and we must ensure we continually move our programs forward to help protect patients.

Appendix 1 – Case Studies in Supply Chain Security Breaches

Valsartan—Supply Chain Contamination. In January 2019, the US Food and Drug Administration reported that some generic versions of angiotensin II receptor blocker (ARM) medicines contain nitrosamine impurities that don't meet the agency's safety standards. ARBs, including valsartan, irbesartan, losartan and others, are a class of medicines used to treat high blood pressure and heart failure. Nitrosamine impurities, including N-Nitrosodimetheylamine (NDMA) and N-Nitrosodiethethylamine (NDEA) are probable human carcinogens. This issue surfaced in the summer of 2018, when the FDA was informed that API manufactured by Zhejiang Huahai Pharmaceutical Co., Ltd. (ZHP), in Linhai, Taizhou Zhejiang China for some generic valsartan-containing medicines contained NDMA, posing a potential safety concern. The FDA investigation identified that a change made to the manufacturing process likely led to this impurity and that the impurity went undetected by global regulators, including the FDA, for a period of time. Based on May 2019 FDA laboratory testing results and records from manufacturers of the recalled valsartan lots, impurities may have been present in valsartan-containing finished drug lots for up to four years. In June 2019, Teva Pharmaceuticals expanded its voluntary recall to include seven additional lots of losartan potassium tablets labeled by Golden State Medical Supply.

Xanax—Counterfeiting. The brand name alprazolam is a benzodiazepine drug widely prescribed to treat anxiety disorders and panic attacks is another drug that has been counterfeited because of market demand. In a 21-month period (2015-2017), it was estimated that more than 1.5 million counterfeit Xanax pills were sold in Britain. The counterfeits were dangerous and found to be laced with everything from acid and heavy metals to floor polish. In a report dated Feb 25, 2019 entitled 'Fake Xanax on the rise' Instead of creating a weaker version of the drug, the counterfeit version of Xanax was laced with a deadly synthetic opioid called fentanyl which is a very potent painkiller that is 50 to 100 times stronger than heroin and morphine. The existence of fake Xanax first came to the attention of doctors in late 2015 when users came to the ER with traces of fentanyl in their blood. The doctors suspected that the Xanax pills they took were counterfeit and this was later confirmed when the Xanax pills were tested

Botox—Counterfeiting. In 2015, FDA alerted health care practitioners and the public that a counterfeit version of Botox was found in the United States and may have been sold to doctors' offices and medical clinics nationwide. There were some similarities between the counterfeit Botox products and the FDA-approved Botox for injection (100 units/vial), manufactured by Allergan. An unlicensed supplier (who is not authorized to ship or distribute drug products in the United States) sold the product.

Avastin—Counterfeiting/Diversion. February2012, FDA announced the discovery of counterfeit Avastin in the US supply chain. It made clear that the counterfeits were intertwined with International diversion schemes involving Quality Specialty Products (QSP). The Avastin counterfeit is one example of the dangers of Diversion. Criminals faked Turkish Avastin (at least in some cases), not the version approved in the US (Genentech label not Roche). In other words, they were substituting counterfeits for apparently diverted genuine product**.** The Feb 14 FDA posting identified specific doctors and practices that had purchased diverted (or counterfeit) product from QSP. FDA made clear that its concern extends to illegal importation and use of unapproved foreign medicines, as well as counterfeits.

Lilly Labs Warehouse Burglary—Cargo Theft. In March 2010, a group of sophisticated thieves broke into a Connecticut warehouse owned by Eli Lilly & Company and made off with an estimated $76 million in medications – the biggest recorded cargo theft in history. The stolen medications included flagship brands Prozac, Cymbalta, Strattera, and Zyprexa, and seemed to be the target of the heist, as controlled substances were left untouched. This theft was similar to a 2009 in Richmond, Virginia burglary that occurred, where thieves stole $5.5 million worth of Advair inhalers from a GlaxoSmithKline distribution facility. The method of entry was not typical; thieves cut a hole in the roof, slid down a rope, and disabled the alarm system from the inside of the building. The FDA published a letter soon after the theft was reported, warning customers to purchase the affected brands only from reputable sources.

On October 14, 2011, law enforcement authorities searched a storage facility in Florida and recovered pharmaceuticals that had been stolen from the (Lilly) Enfield warehouse. In 2016, two brothers (among 23 suspects arrested for a series of cargo thefts) plead guilty to charges related to the burglary. Lilly's insurer, National Union of Pittsburgh, claims Amaury and Amed Villa gained access to the company's assessment of the warehouse that showed all of its weak points. "Either they were given access to this data, or there was a weak link that allowed ADT to be hacked," Elisa Gilbert, a lawyer for the insurer has said.

Astellas Truck Hijacking—Cargo Theft. In June 2009, an employee truck driver of Tokyo-based Astellas Pharma pulled off the road into a truck stop to take a shower. When the driver returned, his truck had been stolen. The truck contained 18 pallets with 21 different medicines, including Prograf, an immunosuppressant that depends for its effectiveness on storage in proper temperatures and humidity. Left in a non-controlled environment trailer or warehouse, it can fail resulting in major complications for a transplant recipient.

As discussed above, compromising the "cold chain" is one of the major hidden risks associated with cargo theft. Within a week, Astellas withdrew all the drugs on the marketplace with same lot numbers as those from the stolen load. Pills in drugstores and hospitals nationwide had to be destroyed. While the value of the cargo was only $10 million

by itself, the costs of the recall brought Astellas' total out-of-pocket expenses to $47 million. It wiped out over 10 percent of the company's North America sales for the quarter.

Heparin—Intentional Adulteration. A more recent instance involving true economic adulteration took place in 2008, when contaminated heparin, sourced from China, entered the global supply chain. Most of the world's heparin comes from China, where farmers process pig intestines for ingredients that consolidators and pharmaceutical makers process for export. Over 10 million patients receive heparin annually. Over twelve manufacturers, located all over the globe, unknowingly purchased contaminated heparin sourced from China. One of the companies, Baxter International, accounted for about half the United States' heparin injectable market.

In late 2007 and early 2008, an increase in adverse events was reported in patients receiving heparin, particularly patients undergoing hemodialysis or cardiac procedures. Through a joint investigation by the FDA, Baxter and other industry experts, OSCS was identified as a contaminant in certain lots of heparin. OSCS closely resembled heparin in both chemical structure and anti-coagulant (blood-thinning) properties. A still-unknown third party deliberately (and criminally) selected OSCS precisely because it mimics heparin and would evade detection in state-of-the-art tests. The contaminant was likely added deliberately, possibly to stretch the supply of a profitable export, according to FDA officials.

Viagra & Cialis—Counterfeiting. Also, in 2005, Pfizer and Lilly's erectile dysfunction drugs were the targets of a counterfeit scheme where drugs were imported from China and distributed domestically. In connection with the work on the case, Chinese officials recovered 600,000 counterfeit Viagra labels and packaging, 440,000 counterfeit Viagra and Cialis tablets, and 260 kilograms of raw materials used to manufacture counterfeit drugs.

Tylenol—Intentional Adulteration. While something of a one-off due to the lack of economic motivation behind the incident, the financial impact of the 1982 Tylenol murders has been thoroughly studied by analysts and academics and contains perhaps the most detailed data among all the case studies. Notably, it presents an evaluation of the staggering impact of the intentional adulteration on a company's – here, Johnson & Johnson's (J&J) – brand value. In his article "The Impact of External Parities on Brand Name Capital: the 1982 Tylenol Poisonings and Subsequent Cases", Mark Mitchell captured this elusive figure, estimating that the decline in value of the J&J and Tylenol brand names following the incident approximated
$1.24 billion.

Appendix 2 – Example of Rx-360 Collaboration

Following the events in Japan on Mar 2011, an Rx-360 working group actively shared information, practices and risk based approaches to help protect patient safety. Common themes for the risk based frameworks were discussed.

Appendix 3: Trends in Pharmaceutical SCS Incidents

PSI has collected data on counterfeiting, illegal diversion and theft incidents for fifteen consecutive years. The yearly totals for the last five years are shown on the adjacent bar chart.

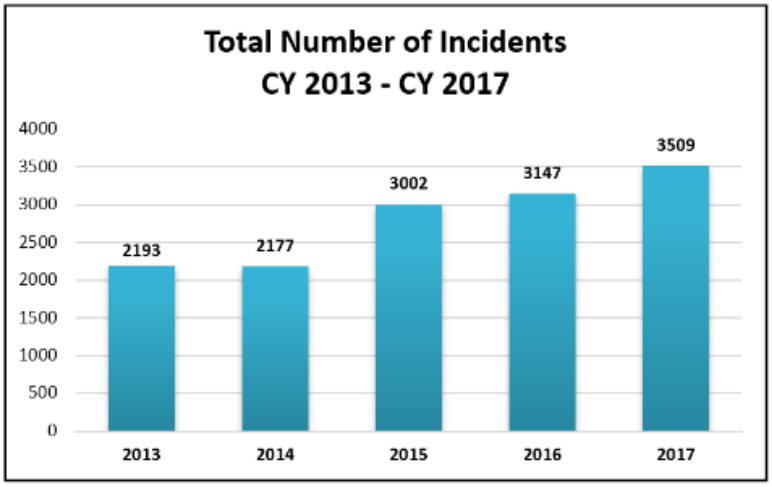
The chart shows:

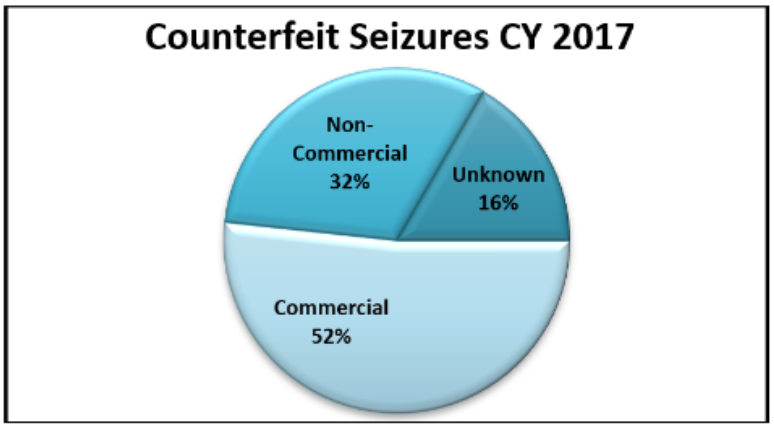
- 3,509 pharmaceutical crime incidents in CY 2017
- Incidents increased by eleven percent increase (+11%) from CY 2016
- Incidents were at an all-time high
- Over the past five years, incidents increased by sixty percent (+60%)

To gauge the magnitude of these counterfeiting incidents, PSI continued to track the quantity of drugs seized. Incidents involving the seizure of more than 1,000 dosage units were classified as a commercial incident; incidents involving less than 1,000 dosage units were classified as non-commercial.

The Institute found:

- 590 counterfeiting incidents involved either customs seizures or police/health inspector raids
- Seizures increased by thirteen percent (+13%) over the prior year
- Thirty-two percent (32%) of the seizures were non-commercial
- Commercial seizures represented fifty-two percent (52%) of the total





Source: Pharmaceutical Security Institute.

Original Source Documentation References

Amir Efrati & Peter Loftus, *Lilly Drugs Stolen in Warehouse Heist*, THE WALL STREET JOURNAL (Mar. 17, 2010)

Barchi Peleg-Gillai, Gauri Bhat & Lesley Sept, *Innovators in Supply Chain Security: Better Security Drives Business Value*, The Manufacturing Institute (July 2006),

http://www.gsb.stanford.edu/scforum/documents/Innovators_in_SC_Security.pdf

Daniel Grushkin, *Cargo Theft: The New Highway Robbery*, BLOOMBERG BUSINESSEEK (May 26, 2011)
Ian Yarett, *The $75 Million Pharmaceutical Heist*, NEWSWEEK (Mar. 16, 2010)

James B. Rice & Philip W. Spayd, *Investing in Supply Chain Security: Collateral Benefits*, Special Report for the IBM Center for the Business of Government (May 2005)

JDS Uniphase Corporation, *Pharmaceutical Counterfeiting, Tampering, and Diversion: Solutions for Addressing a Growing Threat*, White Paper (Mar. 2010)

Justin Rohrlich, *What the Eli Lilly Theft Means for Pharm*a, Minyaville.com (Mar. 17, 2010)

Kodak Corporation, *Brand Protection Strategies: Defending Against Gray Market Diversion*, Executive White Paper,
http://graphics.kodak.com/KodakGCG/uploadedFiles/Products/Security_and_Authentication/K-162_GrayMkt_WhtPpr_0610_lo.pdf

Larry Rosania, *Heparin Crisis 2008: A Tipping Point for Increased FDA Enforcement in the Pharma Sector?*, 65 FOOD & DRUG L.J. 489 (2010)

Marcel GAM Moester, *Counterfeit Medicine Case Studies from the Netherlands and the UK*, 14 EJHPPractice 62-64 (2008)

Patricia Van Arnum, *Navigating the Global Pharmaceutical Supply Chain*, Pharmtech.com (Mar. 2, 2010)

Statement of Deborah M. Autor Before the Committee on Health, Education, Labor and Pensions, Securing the Pharmaceutical Supply Chain (Sept. 14, 2011)

Stephanie Sutton, *Counterfeiting to Reach Worst Rates Yet This Year*, Pharmtech.com (Jan. 7, 2011)

Updated Links

1. https://www.pewtrusts.org/~/media/legacy/uploadedfiles/phg/content_level_pages/issue_briefs/casestudyunsafedrugsv2pdf.pdf

2. http://www.cnn.com/2012/03/15/health/margaret-hamburg-fda-medication-labels/index.html

3. http://www.pharmatimes.com/web_exclusives/the_escalating_pharma_counterfeit_problem_1271942

4. https://www.fda.gov/drugs/drug-safety-and-availability/counterfeit-version-botox-found-united-

states

5. https://www.safemedicines.org/2016/08/dea-considers-fentanyl-containing-counterfeit-medications-a-global-threat.html
6. https://www.justice.gov/usao-ct/pr/citizen-cuba-sentenced-7-years-prison-eli-lilly-theft-additional-multimillion-dollar
7. https://anaheimlighthouse.com/blog/fake-xanax-on-the-rise/
8. https://www.fda.gov/drugs/drug-safety-and-availability/fda-updates-and-press-announcements-angiotensin-ii-receptor-blocker-arb-recalls-valsartan-losartan
9. https://www.fda.gov/drugs/drug-safety-and-availability/laboratory-analysis-valsartan-products
10. http://www.psi-inc.org/incidentTrends.cfm
11. http://www.pharmatimes.com/web_exclusives/the_escalating_pharma_counterfeit_problem_1271942
12. http://www.pharmatimes.com/web_exclusives/the_escalating_pharma_counterfeit_problem_1271942
13. https://www.fiercepharma.com/supply-chain/trial-lilly-warehouse-burglary-raises-security-questions-for-pharma
14. https://www.justice.gov/usao-ct/pr/citizen-cuba-sentenced-7-years-prison-eli-lilly-theft-additional-multimillion-dollar
15. https://www.fda.gov/drugs/drug-safety-and-availability/counterfeit-versions-cialis-tablets-identified-entering-united-states
16. https://www.adn.com/alaska-news/crime-courts/2017/07/19/safeway-to-pay-3-million-for-drug-theft-reporting-problems-first-detected-at-wasilla-carrs/
17. https://www.fda.gov/drugs/drug-supply-chain-integrity/drug-supply-chain-security-act-dscsa
18. https://ec.europa.eu/health/human-use/falsified_medicines_en