THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

VOLUME 9 NUMBER 6

DECEMBER 2010

Postal and Shipping Sector

Editorial Staff

Editors
Devon Hardy
Olivia Pacheco

Staff Writers
M. Hasan Aijaz
Shahin Saloom

JMU Coordinators
Ken Newbold
John Noftsinger

Publisher
Liz Hale-Salice

Contact: dhardy1@gmu.edu
703.993.8591

Click **here** to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

In this month's issue of *The CIP Report*, we highlight specific topics that affect the Postal and Shipping Sector. The events that occurred in October 2010 underline the importance of this Sector, especially during the holiday season.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

We feature an article from the President of The Berkshire Company, who provides recommendations to mail centers to enhance their security. The President of the Cargo Intelligence and Security Association and the Chairman of Powers Global Holdings discuss the capabilities of smart containers in protecting the global supply chain. Then, the impact of piracy on shipping and global trade is examined. Finally, we provide a brief overview and update on the events that occurred in October 2010, in which two toner-cartridges carrying explosive material were shipped to the United States from Yemen.

This month's *Legal Insights* analyzes the initiatives that have been launched by the United States Customs and Border Protection (CBP) to ensure secure and efficient trade.

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

Mail Center Security: Handling With Care

by Mark Fallon, President and CEO, The Berkshire Company

"Want of care does us more damage than want of knowledge."

– Ben Franklin

In July 2010, a package bomb disguised as a box of chocolates was sent to an oil executive's home in Houston, Texas. In October 2010, terrorists shipped package bombs labeled as copier parts. During the month of November, Italy and Greece saw an increase in the number of parcel bombs.

The proper response to these incidents is a renewed dedication to preparedness. Security in mail centers is always important, and the holiday season is no exception. Increased volumes of packages and a festive atmosphere can lead to a lax attitude. Managers must take a proactive approach towards security and awareness by reinforcing the basics, reexamining current plans, and increasing the amount of training. The following recommendations are provided to improve mail center preparedness.

It is essential that mail centers review security plans and make certain that it includes measures to protect employees from harm and safeguard the mail that is handled. Also, the physical layout of mail centers should be examined. Mail centers should also ensure that all access points are secured from unauthorized entry. In addition, non-mail operations employees should be prohibited from entering the mail center to pick up mail or packages. Furthermore, a service counter should be contructed to handle queries from customers (an inexpensive and effective solution is to put a table in front of mail centers).

The service counter and all doors should be monitored by surveillance cameras —— an excellent deterrent. However, surveillance cameras make some people uneasy. Employees should be informed that the cameras are used to help protect them from harm. Open, honest communication is essential for a security plan to be successful.

Openness with employees should be easy because a background check should have already been conducted before they were hired. If this has not already occured, it is important to work with human resources to establish a screening process for all employees. If an outsourcing vendor is used, background checks on their staff should also be required.

Employees must be trained to recognize a suspicious package or envelope. The characteristics of a potential hazard include:

- No Return Address
- Excessive Postage
- Misspelled Words
- Protruding Wires
- Strange Odor
- Oily Stains/Discoloration on Wrapper
- Excessive Tape or String

Letter bombs do not fit in a flat envelope. Therefore, if feasible, purchase an x-ray machine. An x-ray machine can easily detect the components of a letter bomb. All employees should be trained on how to properly use the x-ray machine, and how to react if they detect a threat.

It is crucial to communicate and post procedures on how to handle an envelope or a package that contains a threat of a biological or chemical agent, or an unidentified powdery substance. The United States Postal Inspection Service uses the acronym "SAFE:"

Safety comes first.
Assess the situation before taking action.
Focus your efforts on the hazard, avoiding contact and access.
Evaluate the situation and notify authorities.

The most important thing to remember when dealing with a mail bomb, or biological or chemical agent threat is: do not panic. Rash actions can lead to even more harmful consequences. Bombs sent through the mail do not usually have ticking timers, and biological agents do not spread rapidly on their own. If a mail center receives a suspicious package, cordon off the area and follow the established procedures:

(Continued on Page 9)

The Private Sector's Contribution to Security and Efficiency

by Ed Harrison, President, Cargo Intelligence and Security Association, and
Dr. Jim Giermanski, Chairman, Powers Global Holdings

Most supply chain executives understand that smart containers can detect something, but little more is known or appreciated. In fact, not all smart containers have the same levels of intelligence. The smartest type tells who supervised its stuffing, what is in it, where it is leaving from and where it is going, who is carrying it, where it is at any given time, where it is and should not be, and whether an authorized person opens it at destination. It will also signal any unauthorized access en-route and say where that access took place. The least intelligent container usually can tell you if its doors were opened en-route.

There is also the issue of government and non-government compliance. To comply with most programs today a smart container consists of an *end-to-end, door-to-door, origin-to-destination* security and supply chain optimization system that meets or exceeds the requirements and benefits of World Customs Organization (WCO) Standards; the United Nation's (UN) Single Window concept, through which electronic data flows. Smart containers also meet the requirements of security programs such as the Customs Trade Partnership Against Terrorism (C-TPAT); the Authorized Economic Operator (AEO); and multiple legislative acts of different nations, to include changes in the U.S. Federal Rules of Civil Procedures with respect to the qualification and use of electronic evidence as part of a chain of custody.

Recently Alan Bersin, Commissioner, U.S. Customs and Border Protection (CBP), U.S. Department of Homeland Security (DHS), before the Senate Commerce, Science and Transportation Committee, supported the importance of technology:

We are operating in the age of integrated global supply chains, and our approach to this environment must be equally comprehensive and global. While inspections and operations at our ports are a key component of our strategy, to fully meet our responsibilities, we must identify and stop threats before they arrive at American ports. This requires that we secure the flow of cargo at each stage of the supply chain — at the point of origin, while in transit, and when it arrives in the United States.

This move toward technology is also internationally supported. The first support for an "electronic" supply chain actually began with the Revised Kyoto Convention of 1999. This Convention developed guidelines for the use of advanced electronic transmission of information to Customs' computerized systems, including the use of electronic exchange of information for export and import transactions.[1]

This was the first organizational step moving the global supply chain toward the "electronic age." It was soon followed by a series of agreements and laws further defining the use and implementation of electronic data:

1. U.S. Trade Act of 2002 as amended by The Maritime Transportation Security Act;

2. UN Commission for Europe Recommendation 33-Single Window (2004);

3. U. S. Customs and Border Protection's (CBP) Customs Trade Partnership Against Terrorism (C-TPAT);

4. The U.S. Automated Commercial Environment and E-Manifest Systems;

5. Kyoto Convention ICT Guidelines (Information and Communication Technology) 2004;

(Continued on Page 10)

[1] http://www.wcoomd.org/home_pfoverviewboxes_tools_and_instruments_pfrevisedkyotoconv.htm.

Piracy in Africa and the Shipping Industry

Introduction

Since the beginning of ancient civilization, societies have navigated ocean, coastal, and inland waterways to explore, migrate, and, perhaps most importantly, trade.[1] The International Maritime Organization (IMO) estimates that the shipping industry transports over 90 percent of global trade. In 2008, this was equivalent to 8.17 billion tons of goods.[2] However, the oceans are also a "theater of conflict," a safe haven for drug traffickers, human smugglers, and professionals in one of the world's oldest vocations: piracy.[3] Since 2007, a majority of piratical attacks have occurred in the Gulf of Guinea in West Africa and the Gulf of Aden, which lies between northern Somalia and Yemen. Unfortunately, the Gulf of Guinea and the Gulf of Aden are also strategic global shipping lanes. To further complicate the matter, according to the UN Review of Maritime Transport, "in tandem with the global economic downturn and reduced trade, growth in international seaborne trade decelerated in 2008, expanding by 3.6 percent as compared with 4.5 percent in 2007."[4]

The coasts of Africa have historically been essential to international trade. The Suez Canal, which connects the Mediterranean Sea to the Red Sea off the coast of East Africa, is one of the most important waterways in the world. Its importance stems from the fact that it "provides the shortest maritime route between Europe and the lands lying around the Indian and western Pacific oceans."[5] It is estimated that over 20,000 vessels pass through the Gulf of Aden, carrying a third of the world's crude oil. In 2008, an estimated 3.5 million barrels per day (bbl/d) traveled through the Bab el-Mandab strait, an oil transit chokepoint between the Gulf of Aden and the Red Sea.[6] The country of Nigeria, which is situated on the Gulf of Guinea in West Africa, currently supplies 15 percent of oil imports to the United States. In 2015, this number is expected to increase to 25 percent.[7] Therefore, not only are these regions significant sources of revenue for Africa, they also supply a considerable amount of resources, especially oil, to the United States. Unfortunately, these strategic waterways have witnessed an increase in piracy. According to the International Maritime Bureau (IMB), this is a result of the "increased ability of the pirates to attack vessels further out at sea as well as being better armed, organized, and last but not least the lack of proper law enforcement."[8]

Recent Statistics

In 2009, the IMB Piracy Reporting Centre recorded 406 actual and attempted pirate attacks. This was an increase from the previous year, in which 203 actual and attempted attacks were recorded. Of the 406 attacks, 211 occurred in the Gulf of Aden, the Red Sea, and off the coast of Somalia. The IMB attributed these attacks to Somali pirates. The remaining attacks occured in various locations around the world. According to the IMB, Somali pirates were also responsible for six

(Continued on Page 5)

[1] International Maritime Organization, available at: http://www.imo.org/About/Pages/Default.aspx.
[2] United Nations, *Review of Maritime Transport*, (United Nations: New York and Geneva, 2009), 23.
[3] Scott B. Borgerson, *The National Interest and the Law of the Sea*, Council on Foreign Relations, (New York, NY: May 2009), 14.
[4] United Nations, *Review of Maritime Transport*, (United Nations: New York and Geneva: 2009), xiv.
[5] Suez Canal Authority, accessed August 14 at www.suezcanal.gov.eg.
[6] Dennis W. Sampson, *USAFRICOM's Role in Counter-Piracy Operations in the Horn of Africa*, Naval War College, (Newport, RI: May 2009), 3.
[7] David L. Goldwyn and J. Stephen Morrison, *A Strategic U.S. Approach to Governance and Security in the Gulf of Guinea: A Report of the CSIS Task Force on Gulf of Guinea Security*, Center for Strategic and International Studies, (Washington, DC: July 2005), 5.
[8] International Chamber of Commerce, International Maritime Bureau, *Piracy and Armed Robbery against Ships, Report for the Period 1 January – 31 March 2010*, (Kuala Lumpur: 2010), 24.

Piracy and Shipping *(Cont. from 4)*

attacks in the Arabian Sea, the Indian Ocean, and off the coast of Oman.[9] A recent report by the IMB estimates that from January to September 2010, Somali pirates were responsible for 44 percent of the 289 world-wide recorded attacks.

However, the IMB claims that attacks by Somali pirates are occurring further out to sea. This coincides with the revelation that attacks in the Gulf of Aden have, thus far, decreased. The IMB asserts that pirate attacks have decreased in the Gulf of Aden because international navies are regularly patrolling the waters around the Horn of Africa and shipping vessels have implemented anti-piracy measures. However, the number of hijackings has slightly increased from last year. In addition, pirate attacks have increased in the former piracy hot-spot, the South China Sea.[10]

It is important to keep in mind that maritime statistics are not universal. While the IMB and the IMO are legitimate databases and are often referred to in academic literature and government documents, given that the definition of piracy has been evolving since pirates first sailed out of the mist, the statistics on the number of pirate attacks vary within organizations.

Cost of Piracy

In general, it is difficult to estimate the cost of piracy on the global economy. This is commonly attributed to the fact that experts do not agree on how to measure the cost of piracy. Some experts argue that "class actions and claims by crew and their unions, strikes, refusals to sail, increased employee insurance premiums claims and demands for higher wages" must be considered.[11] Others argue that the expense of stolen cargo, goods, and ships; delays in port; alternative trading routes; and increased wages for crew sailing in pirate prone waters should all be considered when estimating the cost of piracy. An increase in insurance rates is also often considered when calculating the cost of piracy.[12] For example, in May 2008, Lloyds of London designated the Gulf of Aden a "war-risk" zone subject to a special insurance premium.[13] Hence, estimates on the exact cost of piracy vary greatly. In literature and government documents, estimates range from $1 billion to $16 billion a year[14] or $500 million and $25 billion per year.[15]

There is also debate about the impact of piracy on the global economy. While some experts discern that the impact of piracy on the global economy is astronomical, some argue that since the likelihood of a ship being successfully attacked is relatively low, piracy should not be considered a global menace. For example, participants at a RAND Workshop argued that "piracy does not pose a threat to international maritime trade, much less to the global economy. Piracy is a regional problem, the effects of which fall disproportionately on those states that are most severely affected by the phenomenon, namely Somalia, Nigeria, Indonesia, Tanzania, India, and Bangladesh."[16] As a result, there is concern that the naval response to piracy in the Horn of Africa is exaggerated, unnecessary, and, most importantly, a misallocation of resources.

On the other hand, some experts

(Continued on Page 11)

[9] These statistics are derived from the International Chamber of Commerce International Maritime Bureau, *Piracy and Armed Robbery against Ships Annual Reports*, (1 January to 31 December 2009), (Kuala Lumpur, Malaysia).

[10] International Chamber of Commerce, *Pirates Intensify Attacks in New Areas, with First Somali Hijacking Reported in Red Sea*, (October 18, 2010).

[11] Matt Elbeck, "The Threat of Piracy on Maritime Transportation," *International Journal of Society Systems Science*, 2:2 (2010), 129.

[12] Donna Nincic, "Maritime Piracy in Africa: The Humanitarian Dimension," *Africa Security Review*, 18:3 (Institute for Security Studies, September 2009), 13.

[13] Lauren Ploch, Christopher M. Blanchard, Ronald O'Rourke, R. Chuck Mason, and Rawle O. King, *Piracy off the Horn of Africa*, (Washington DC: Congressional Research Service, 2009), 2.

[14] Helen B. Bendall, "Cost of Piracy," *Maritime Economics and Logistics*, 12:2 (2010), 182; and Stephanie Hanson, *Combating Maritime Piracy,* Council on Foreign Relations, (January 2010).

[15] Lesley Ann Warner, "Pieces of Eight: An Appraisal of U.S. Counterpiracy Options in the Horn of Africa," *Naval War College Review*, 63:2 (Spring 2010), 65.

[16] Peter Chalk, Laurence Smallman, Nicholas Burger, *Countering Piracy in the Modern Era: Notes from a RAND Workshop to Discuss the Best Approaches for Dealing with Piracy in the 21st Century,* (RAND Corporation, 2009), 2.

Air Cargo Security

In response to the attempted bombing on Northwest Airlines Flight 253 on Christmas Day 2009, the United States joined the International Civil Aviation Organization's (ICAO) Declaration on Aviation Security on October 8, 2010. The Declaration on Aviation Security addresses the shared responsibility between the United States and the European Union (EU) "to prevent terrorists and serious criminals from conducting, planning, and supporting operations with the intention to cause harm to our populations including by exploiting civil aviation, while upholding the rule of law and observing and promoting respect for international law, including international human rights law."[1] The Assembly recognizes that aviation security is international in nature and therefore requires a collaborative effort to counter threats by "developing and implementing strengthened and harmonized measures and best practices for air cargo security."[2]

During the week of October 25, 2010, two toner-cartridges carrying explosive material called Pentaerythritol tetranitrate (PETN) were shipped to the United States from Yemen. PETN is a highly explosive organic compound belonging to the same chemical family as nitroglycerin.[3] PETN was also the same material used in the bomb that Umar Farouk AbdulMutallab attempted to ignite aboard Northwest Airlines Flight 253 as it approached Detroit, Michigan, on December 25, 2009.[4] Fortunately, both shipments were intercepted in the United Kingdom (UK) and the United Arab Emirates (UAE). John Brennan, Assistant to the President for Homeland Security and Counterterrorism, stated that the discovery of the packages was the result of the Kingdom of Saudi Arabia sharing information, and the UK and the UAE's ability to identify suspicious packages.[5]

The U.S. Transportation Security Administration (TSA) and U.S. CBP responded to the situation by grounding packages from Yemen and deploying a team of inspectors to assist the Yemen government with their cargo screening procedures.[6] TSA Administrator John S. Pistole met with Yemeni Deputy Prime Minister Rashad al-Alimi and aviation officials and toured a cargo facility in Sana'a.[7] In addition, Pistole met with international aviation security officials and signed an international security agreement with Germany. This agreement will "enhance the sharing of aviation security best practices…(and) will help facilitate mutual aviation security goals to harmonize measures that continue to ensure the safety of travelers."[8]

On November 3, 2010, DHS Secretary Janet Napolitano spoke with international shipping companies, including Federal Express (FedEx) and United Parcel Service Inc. (UPS), to discuss methods of strengthening air cargo screening on their planes and implementing "preventative measures, including terrorism awareness training for personnel."[9] Secretary Napolitano also contacted General Giovanni Bisignani, Director of the International Air Transport Association (IATA), to reiterate her commitment to ongoing coordination between the airline and shipping industries and ways "to protect the global supply

(Continued on Page 13)

[1] http://www.dhs.gov/ynews/releases/pr_1264119013710.shtm.
[2] http://www.tsa.gov/press/releases/2010/1103.shtm\.
[3] http://www.britannica.com/EBchecked/topic/454067/PETN.
[4] http://www.politico.com/news/stories/1209/30980.html.
[5] http://www.whitehouse.gov/the-press-office/2010/10/29/statement-john-brennan-assistant-president-homeland-security-and-counter.
[6] http://www.tsa.gov/press/releases/2010/1103.shtm.
[7] Ibid.
[8] Ibid.
[9] http://www.dhs.gov/ynews/releases/pr_1288810245939.shtm.
[10] http://thompsonahern.blogspot.com/2010/11/dhs-steps-up-cargo-screening.html.

Legal Insights

Custom and Border Protection's Initiatives to Ensure Secure and Efficient Trade

by Hasan Aijaz, J.D.

The Postal and Shipping Sector presents a challenge in ensuring that no dangerous or illegal materials enter the United States while maintaining efficient transportation of goods across the Nation's borders. The United States CBP is the "single, unified border agency of the United States;"[1] it helps to protect U.S. citizens against dangerous people and objects from entering into the United States. This mission is of high strategic importance; however it must be performed "without stifling the flow of legitimate trade and travel that is so important to our Nation's economy."[2] Thus, the CBP ensures borders are both efficient and secure. The challenges facing CBP in meeting these missions are immense; CBP processed more than 350 million individuals, 25 million trade entries, and examined over 5 million containers in 2009.[3] In order to surmount these challenges, CBP administers a number of programs to achieve these goals, including the C-TPAT, the Free and Secure Trade Program (FAST), and the Cargo Security Initiative (CSI).[4] These programs are used to increase the efficiency of trade while maintaining security.

C-TPAT was initiated in April 2002. It was formed in response to the events of September 11, 2001 to implement an effective means of protecting the United States "against acts of terrorism by improving security while simultaneously speeding the flow of compliant cargo and conveyances."[5] C-TPAT is a voluntary program between government and business designed to "strengthen and improve overall international supply chain and U.S. border security."[6] Participation in C-TPAT allows companies to be designated as low-risk and "therefore less likely to be examined" when transporting goods into the United States. C-TPAT is open to "importers, carriers, freight forwarders, customs brokers, U.S. port authorities, terminal operators and Mexican and other CBP-invited foreign manufacturers."[7]

In order for industry partners to be certified with C-TPAT, they must pass a rigorous assessment process which looks at the totality of their supply chain in order to ensure that the partner is qualified for low-risk treatment when importing goods into the United States. Among factors that are examined when undergoing C-TPAT certification are topics such as "personnel, physical and procedural security; access controls; education, training and awareness; manifest procedures; conveyance security; threat awareness; and documentation processing."[8] Compliance with requirements is based upon a self-assessment which is submitted to

(Continued on Page 8)

[1] Statement of Robert C. Bonner, Commissioner CBP, Hearing before the Permanent Subcommittee on Investigations, Senate Committee on Homeland Security and Governmental Affairs (May 26, 2005).
[2] Ibid.
[3] Testimony of Todd Owen, Executive Director, Cargo and Conveyance CBP, Before Science and Technology Committee (November 17, 2009).
[4] See statute at 6 USC § 968.
[5] *Securing the Global Supply Chain: Customs-Trade Partnership Against Terrorism (C-TPAT Strategic Plan)*, Customs and Border Protection, available at http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/what_ctpat/ctpat_strategicplan.ctt/ctpat_strategicplan.pdf (last accessed November 10, 2010).
[6] http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/what_ctpat/ctpat_overview.xml (last accessed November 9, 2010).
[7] *Terminal Operators and Their Role in U.S. Port and Maritime Security*, Congressional Research Service (April 2007).
[8] Ibid.

Legal Insights *(Cont. from 7)*

CBP and may then be verified with site visits. A partner must have appropriate controls in these areas in its own operation and must focus on bringing their partners and service providers into compliance with the requirements. C-TPAT participants must agree to abide by these requirements in order to maintain their low-risk status. A certified C-TPAT partner thus represents a secure and dependable supply chain from product origination to is final destination into the United States.

C-TPAT partners must undergo a certain amount of cost and procedural change in order to be certified. These costs include developing new procedures, complying with physical security requirements (such as installing lighting, cameras, fences, etc.) and costs involved in maintaining these systems and procedures. However, C-TPAT participants benefit by their interaction with CBP. The benefits of C-TPAT participation include reduced number of inspections, shorter wait times, and opportunities to participate in CBP security training seminars. Participation in C-TPAT is also beneficial to industry partners as it reduces the chances of supply disruption (by minimizing risk) and increases efficiency.

The mutual benefits of the C-TPAT can be seen by the participation of over 8,000 partners, which includes more than 80 percent of the top 100 importers into the United States.[9] For the United States and CBP, one of the primary successes of the C-TPAT has been in enabling CBP to broaden its influence beyond its regulatory reach. The CBP does not have any jurisdiction in foreign ports, but by creating partnerships with the private companies that operate from those ports, CBP is able to influence behavior and increase the security of goods flowing in from those ports.[10]

The FAST program is a "commercial clearance program for known low-risk shipments entering the U.S. from Canada and Mexico."[11] It is a complementary program to C-TPAT because participation in FAST "requires that every link in the supply chain, from manufacturer to carrier to driver to importer" has been certified under the C-TPAT program. Registration to the FAST program requires an applicant to register with the Global Online Enrollment System (GOES) website or through paper applications. The FAST program is in use with over 100,000 drivers who have been enrolled in the FAST program at 55 land border ports[12] and is the first paperless cargo release mechanism administered by CBP.[13]

The FAST program is administered under two heads, one agreement between the United States and Canada, and a separate agreement with the United States and Mexico. FAST North is the United States/Canada component and FAST South is the United States/Mexico component; both are designed to further CBP's mission with a special emphasis to "ensure security and safety while enhancing the economic prosperity of both countries."[14] The FAST program expedites clearance of cargo and streamlines the registration for drivers, carriers, and importers which "minimiz[es] paperwork" for low risk companies and individuals.[15] Added benefits include, dedicated lanes at certain ports, reduced examinations, and a head start on modifications to the program.[16]

The CSI program was another

(Continued on Page 12)

[9] Based on "containerized cargo volume" Id at 13, see also Customs-Trade Partnership Against Terrorism 2010 Partner Survey, Center for Survey Research, available at http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/ctpat_survey.ctt/ctpat_survey.pdf (last accessed November 15, 2010).

[10] See Testimony of Todd Owen, Executive Directory, Cargo and Conveyance Security CBP, DHS on November 17, 2009, available at http://gop.science.house.gov/Media/hearings/oversight09/nov17/Owen.pdf (last accessed November 15, 2010).

[11] http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/travel/fast/fast_fact.ctt/fast_fact.pdf (last accessed November 9, 2010.

[12] Free and Secure Trade, CBP, available at http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/travel/fast/fast_fact.ctt/fast_fact.pdf (last accessed November 15, 2010).

[13] U.S./Canada FAST Program Overview, CBP, available at http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/fast/us_canada/us_canada_information.ctt/us_canada_information.doc (last accessed November 18, 2010).

[14] Ibid.

[15] Ibid.

[16] Ibid.

Mail Center Security *(Cont. from 2)*

• Isolate the package. Do not have people gather to look at the package. This procedure holds true for any suspicious package.

• Do not "test" the package by shaking it, or tasting a substance.

• Alert other employees that a suspicious package has been found, and that they should remain clear of the area.

• Note the specific points that make this package suspicious.

• Write down all available information from each side of the item (names, addresses, postmarks, labels, markings, etc.).

• Have someone call 911. Tell the dispatcher what has been received and what has been done with it. Also, contact the firm's security office.

• Call the local postal inspector.

• Wash hands with soap and warm water for one minute.

• If a biological agent is suspected, do not allow anyone to leave the office that might have touched the package.

• When emergency responders arrive, they will provide further instructions.

In this situation, mail centers should be prepared to answer many questions from the emergency responders. The police and postal inspectors have extensive knowledge of bomb and biological threats. Their questions and the responses of mail centers will help determine the next steps for handling the threat.

The actions taken during a threat have an immediate impact on the safety of everyone in mail centers. The actions taken before a threat have a lasting impact on the safety of everyone in a company. Hence, preparing mail centers and employees to handle a threat is an obligation that must be met every day.

Education and awareness are the most important ingredients to preparedness. Most people have a fear of the unknown. Information is the counter to ignorance and understanding is the precursor to calm. However, being calm is not the same as being casual. Employees must remain aware of their surroundings and the packages they handle. Security programs must be carefully designed and vigorously monitored to reduce the risk for all.

In addition to educating employees who work directly with managers, employees working in the company should also be educated. Employee awareness of the measures that have been taken leads to confidence in the safety of the packages that are delivered to their desktops. It is vital to work with company's security and human resource departments to schedule ongoing training for all current employees. Mail security should be a mandatory briefing for all new employees.

When security programs are developed, contact local police and emergency departments to review the plan, and if possible, ask them to conduct training for your staff. Additionally, request additional materials for training, such as the latest warnings issued to law enforcement. Managers should also ensure that employees have the correct telephone number for the closest hazardous materials (HAZMAT) unit.

As always, use the resources of local postal officials. The United States Postal Inspection Service has been tracking and solving letter bomb crimes since the early 1900s. Responding to 177 different threats and hoaxes involving biological agents from 1999-2000, the postal inspectors were on the front lines of the investigations into the 2001 anthrax attacks. They are also developing countermeasures to reduce the vulnerability of the United States Postal Service and the mail.

The security of mail centers is important, especially during the holidays. While the threat to managers and their employees is minimal, it is real. Mail centers should not fall prey to fear or take rash actions that may create a crisis. Instead, managers should educate themselves and their employees. Develop a sound plan and have it reviewed by experts. Remain vigilant and conduct regular evaluations. Be safe. ❖

Mark Fallon is President and CEO of The Berkshire Company. He may be reached at 508-485-9090, or visit his website at www.berkshire-company.com.

Smart Containers *(Cont. from 3)*

6. World Customs Organization (WCO) Framework of Standards to Secure and Facilitate Global Trade 2005;

7. U.S. Safe Port Act 2006;

8. U.S. Implementing Regulations of the 9/11 Commission Act of 2007;

9. International Standards Organization (ISO) 28000, 2007;

10. U.S. Ten + Two Program; and,

11. The European Union's (EU) Authorized Economic Operator Program.[2]

Technology today can provide the following system and process:

• First, it provides the electronic equivalence of a receipt showing evidence of shipping. This evidence is provided by a specialized electronic data key only usable with and by an authorized individual at the point of origin. That person is identified as the authorized person supervising the stuffing (loading) of the container, and verifying its contents. At the time the electronic data key is inserted into the system in the container, there is a data transfer of the identity of the authorized agent accountable for the verification of the cargo, logistics, and booking information from the shipper, information for Customs Authorities of both outbound and inbound countries as required, and the activation of the system;

• Second, this system provides a unique identifier for tracking. This allows the consignee or consignor not only to query the container but also allows the container to report independently any movement off its intended journey;

• Third, it offers the capacity to serve as a third-party record of the transaction recorded automatically by a worldwide call center;

• Fourth, it provides an electronic receipt of delivery, accomplished by the opening of the container by a person at the point of destination approved and authorized to open the container, which is provided by another specialized electronic data key usable only with and by an authorized individual at the point of destination; and

• Fifth, it offers breach detection into the container not just through the doors, but through any part of the container, off-course alerts, and sensory information such as temperature, humidity, vibrations, and in 2011, in-container radiation sensing that can detect shielded highly enriched uranium, or other sensors as needed by the user.

So far, there are varying claims of benefits to the private sector for using smart containers and their associated technologies and systems. A recent study from Stanford University points to quantifiable benefits such as a 50 percent increase in access to supply chain data, a 38 percent drop in theft and similar losses, a 14 percent cut in excess inventory, and 29 percent reductions in overall transit times. Consulting firm BearingPoint has calculated benefits of up to $700 per container per move while the U.S. Congressional Budget Office has noted savings of 0.8 percent of the value of a smart container's contents.

But the business benefits are only part of what smart containers can do. They also offer enormous potential to improve national security worldwide. Clearly, it is the future that not only makes the supply chain more visible, efficient, and effective for industry, but also safer for all of us. ❖

Contact:
Ed Harrison
President Cargo Intelligence and Security Association
eharrison@powersintlinc.com

Dr. Jim Giermanski
Chairman Powers Global Holdings
powersintnlinc@bellsouth.net

[2] For a comprehensive treatment of this global development of supply chain security, see Dr. Jim Giermanski, "The Development and Globalization of Container Security," *Defense Transportation Journal*, *Forum Issue*, September, 2008, pp.16-22.

Piracy and Shipping *(Cont. from 5)*

view piracy as the beginning of an imminently larger problem. In 2007, a report written by the Navy, Marine Corps, and Coast Guard elucidated that the "[e]xpansion of the global system has increased the prosperity of many nations. Yet

Response to Piracy

The international community has proposed several solutions to combat piracy. In 2008, the United Nations Security Council adopted four resolutions (1816, 1838, 1846, and 1851) to address the increase of piracy off the Horn of Africa. In the same year, the United States and international forces began patrolling waters near Somalia. In December 2008, the U.S. National Security Council (NSC) plan, *Countering Piracy off the Horn of Africa: Partnership and Action Plan,* was implemented to suppress piracy, and to preserve the "interests of the global economy, freedom of navigation, Somalia, and the regional states."[18]

In conjunction with international partners, in 2009, the United States (NAVCENT), responsible for the Combined Maritime Forces operating in the Arabian/Persian Gulf, Gulf of Oman, Gulf of Aden, Red Sea, Arabian Sea, and Indian Ocean, established the Combined Task Force 151 (CTF-151) to conduct anti-piracy operations in the Gulf of Aden and the waters off the Somali coast in the Indian Ocean. In January 2009, in support of Resolution 1851, the Bush Administration formed an interagency Contact Group on Piracy off the Coast of Somalia (CGPCS). The CGPCS, co-led by the State Department and Defense Department, is supported internationally.

As is evident, the international community is extremely concerned about piracy. In fact, numerous other solutions have been put into action to combat piracy in Africa and the South China Sea. The key will be to implement a solution that will eliminate piracy and ensure that this ancient threat will not resurface in future horizons.

Conclusion

The threat of piracy has existed for centuries. It is a complicated issue that, as a result of its romanticized history, continues to generate interest. It also continues to generate debate with regards to its definition, statistics, relevance, and solutions. Regardless of its current impact on the global economy and on global security, it is a threat that has never been eradicated.

Throughout history, there is evidence that when one group of pirates is defeated or disappears, the emergence of another group, perhaps in a different location or in a different time, is usually not far behind. In a period of time in which international seaborne trade is at risk, it is essential that the international community continue to collaborate to eliminate piracy. ❖

[17] *A Cooperative Strategy for the 21st Century Seapower* (October 2007), 6.
[18] Lauren Ploch, Christopher M. Blanchard, Ronald O'Rourke, R. Chuck Mason, and Rawle O. King, *Piracy off the Horn of Africa*, (Washington DC: Congressional Research Service, 2009), 19.

Legal Insights *(Cont. from 8)*

initiative launched after September 11th with a focus on promoting safe and efficient entry of goods into the United States. The CSI specifically instituted "various inspections, screening, and scanning measures to be undertaken both at U.S. and foreign ports."[17] As part of this initiative, an Automated Targeting System (ATS) was implemented which automatically reviews all the information available for cargo and generates information based on risk profiles. High risk cargo can then be targeted for more intensive screening and inspection.[18] These procedures were later amended in 2007 and mandated "100 percent screening of cargo containers and 100 percent scanning of high-risk containers originating outside the United States."[19]

The CSI was initially rolled out to the "top twenty foreign ports, as determined by the volume of containers shipped to the United States."[20] Implementation of the CSI required foreign governments to allow the procedures of the CSI to be implemented in their ports, and in return CBP allows those countries to station their custom officials in U.S. ports. The effect is similar to the voluntary nature of the C-TPAT except that it is a government-to-government relationship as opposed to a government to private relationship. This arrangement has the additional benefit of allowing best practices to be developed as customs officials are exposed to a wider variety of procedures and of increasing information exchange.[21]

Once a foreign government has agreed to participate in the CSI program, the foreign government must follow four steps. The first element is the identification of "high-risk" containers through programs such as the ATS, which was discussed above. Once the containers have undergone a risk stratification, they are pre-screened at the foreign ports. Technology is then used to screen high-risk containers via "x-ray machines, gamma ray machines, and radiation detection devices."[22] The fourth element of the CSI is the use of "smarter, more secure containers" so that once a container has undergone these security procedures it will immediately be apparent if the container has been compromised.[23] The sum effect of these elements is that once a container has been screened at a foreign port, it does not have to be rescreened when entering the United States so long as it was shipped in a secure container and shows no signs of tampering.

All three of these initiatives by CBP are designed to achieve the twin goals of facilitating the secure and efficient entry of goods into the United States. These programs cover both the private and government aspects of the supply chain into the United States and therefore represent a comprehensive method of achieving CBP's goals. As technology advances, CBP will need to continue to take a proactive role in adopting and adapting to new methods of screening and risk analysis. The history of these programs demonstrates that Congress is both willing and able to pass legislation to enable CBP to achieve its mission. ❖

---

[17] Jennifer North, "The Ins and Outs of Modern Ports: Rethinking Container Security," 5 *South Carolina Journal of International Law and Business*. 191.
[18] Ibid.
[19] Ibid.
[20] Owen Bishop, "A Secure" Package? Maritime Cargo Container Security After 9/11," 29 *Transportation Law Journal*, 313, 320 (2002).
[21] "The Container Security Initiative: Balancing U.S. Security Interests With the European Union's Legal and Economic Concerns," 13 *Minnesota Journal of Global Trade*, 123, 133.
[22] Ibid.
[23] Remarks of U.S. Customs Commissioner Robert C. Bonner: Center for Strategic and International Studies, available at http://www.customs.gov/xp/cgov/newsroom/speeches_statements/archives/2002/aug262002.xml (last accessed November 20, 2010).

Air Cargo Security *(Cont. from 6)*

chain from terrorist threats."[10]

As a result of the October 2010 attempted attacks, DHS and TSA implemented significant measures to increase air cargo security on passenger aircraft. The United States extended the ban of inbound cargo from Yemen to cargo from Somalia. TSA requires all cargo that is transported on domestic or international outbound passenger aircrafts to undergo security screening. In addition, all cargo flying to the United States on passenger or all-cargo planes must meet TSA security standards. These standards include specific requirements such as how facilities and cargo are accessed, how cargo must be screened, the vetting of personnel with access to cargo, and employee training. In addition, all international inbound aircraft carrying cargo must provide cargo manifest information to CBP prior to arrival on long-haul flights and at wheels-up on flights from Canada, Mexico, and the Caribbean for additional screening upon arrival in the U.S.[11,12]

This image shows a printer toner cartridge with wires and powder found in a package aboard a plane searched in East Midlands, north of London, Friday Oct. 29, 2010. The cartridge shown was found in one of two explosive packages addressed to Chicago-area synagogues and packed aboard cargo jets originating in Yemen. U.S. official said preliminary tests indicated the packages contained the powerful industrial explosive PETN, the same chemical used in the Christmas attack involving a Detroit-bound airliner. *Photo Courtesoy of AP Photo.*

On December 8, 2010, DHS Secretary Janet Napolitano met with leaders from global shipping companies, including FedEx, UPS, DHL, and U.S. Postmaster General Patrick Donahoe, to reiterate the Obama Administration's commitment to strengthening air cargo screening. Napolitano stressed her ongoing commitment to partnering with the shipping industry to enhance screening and preventive measures to ensure that an incident, such as the October 2010 bombing attempt, does not disrupt the supply chain in the future. In addition, Secretary Napolitano emphasized DHS' continued "collaboration with the Federal, State, local, and private sector partners and international allies to secure the global supply chain through a layered security approach to identify, deter and disrupt threats."[13]

Air cargo security is essential to the global supply chain because it helps to minimize the disruption of commerce. Most importantly, ensuring that security measures are in-place when cargo is shipped on passenger planes saves lives. ❖

---

[11] http://www.dhs.gov/ynews/releases/pr_1289237893803.shtm.
[12] http://www.washingtonpost.com/wp-dyn/content/article/2010/11/08/AR2010110806574.html.
[13] http://www.dhs.gov/ynews/releases/pr_1291853480217.shtm.

The Center for Infrastructure Protection works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1