

CASE STUDY #14

OPERATION SAFE COMMERCE ANALYSIS ARRIVES IN PORT

THE PROBLEM— HOW TO ANALYZE FOREIGN SUPPLY CHAINS TO SAFEGUARD CONTAINER CARGO ENTERING THE U.S. FROM INTERNATIONAL DESTINATIONS.

The Department of Homeland Security and the Bush Administration funded a \$28 million dollar grant to over fifteen companies to try innovative security solutions and allow TSA to analyze their supply chains into the U.S. DHS Secretary Tom Ridge said, "Operation Safe Commerce is about building on our capabilities and strengthening each layer of defense. This program provides the resources to find innovative new ways for ports to track and protect cargo entering the U.S. from all over the world". Companies participating with the Port of New York—New Jersey by submitting their supply chain's security solutions included Boeing, Parsons Brinkerhoff, SPC, Innolog, Unisys Karachi, Sara Lee Coffee and Tea Foodservice, L.L. Bean, Atlantic USA, and Unisys Santos, with the Port Authority of New York and New Jersey and Bearing Point managing the project. *How could all these diverse supply chains moving into the Port from all over the world be analyzed to evaluate their specific security solutions?*

THE SOLUTION — USE AN AUTOMATED ASSESSMENT TOOL TO MAKE IT EASIER TO DO A HIGH LEVEL RISK ANALYSIS AND VALIDATE THE EFFECTIVENESS OF THE VARIOUS SECURITY SOLUTIONS.

RiskWatch for C-TPAT was selected as the risk analysis tool used to evaluate the supply chains shipping into the Port of New York—New Jersey. The specific supply chains evaluated came into the Port from Scotland, Brazil, Turkey and Pakistan and involved shipments of everything from coffee beans to airline wings to t-shirts.

Bearing Point and the Port of New York– New Jersey selected RiskWatch as the risk analysis software tool which was used to evaluate each element of the supply chain in conjunction with requirements such as the C-TPAT (Customs Trade Partnership against Terrorism), the Container Security Initiative standards and the BASC (Business Anti-Smuggling Coalition).

The model involves evaluation various assets of the different supply chains including Containers, Wheeled Vehicles, Cargo, Proprietary Information and Personnel. A total of fourteen supply chain nodes were analyzed, including elements such as empty container depots, point of origin, point of stuffing, point of consolidation, foreign inland routes, container storage areas, port of loading, transshipment between ports and the port of discharge.

A basic questionnaire consisting of more than two hundred questions were asked of operators throughout the supply chains and by the analysts. The questionnaires focused on finding vulnerabilities such as Access Control, Emergency & Incident Response, Intrusion Detection, Cargo Controls, Security Systems, Vessel Integrity, Conveyance Security, Restrictions on Drivers, Security Awareness and Security Procedures, and over twenty others.

Relevant threat data was also collected including data on Bomb Threats, Chemical-Biological Threats, Explosions (Major), Smuggling, Stowaways, Terrorist Attacks and Disclosure.



RESULTS —

We hope supply chain security will some day be a requirement for everyone in our industry," said Beth Rooney, manager, port security, PANYNJ. "We are in the process of rigorously testing what we envision as an easy-to-implement, international standard for continuous custody and knowledge of any commercial container shipment's condition and security."

A wide variety of security solutions were assessed and tested as part of Operation Safe Commerce. These included a wide variety of high-technology seals such as a variety of RFID (Radio Frequency Radio Frequency Identification Device) devices, which, are automatic identification methods relying on storing and remotely retrieving data using devices called RFID tags or transponders. An RFID tag is a small object that can be attached to or incorporated into a product, animal, or person. RFID tags contain silicon chips and antennas to enable them to receive and respond to radio-frequency queries from an RFID transceiver. Passive tags require no internal power source, whereas active tags require a power source. Other solutions ranged from GPS (Global Positioning Satellite) devices, fixed readers, handheld readers, and container tracking devices. Scanners for looking at cargo, and test for chemical agents and biological agents were employed as part of suites of security solutions.

Senator Patty Murray (D-Wash.) announced preliminary results from the Seattle/Tacoma portion of the Operation Safe Commerce pilot program in 2004. Senator Murray said, "The 9/11 Commissions noted that initiatives like Operation Safe Commerce have just begun to secure shipping containers. As everyone here knows, it's hard to understate the economic value of our container system, and there are tremendous challenges facing everyone involved in the global supply chain."

"We can't search every container that comes into our country. With about \$750 billion in cargo arriving in more than 6 million containers a year, the haystack is just too big. So instead we've used technology and intelligence to make the haystack smaller and show us which containers pose a security risk. Operation Safe Commerce has allowed us to identify the vulnerabilities at each step in the supply chain, and determine, document and test the best systems to bring cargo containers into our ports every day, using different security methods in different environments. Over the past months it has allowed our nation's three largest ports to monitor and track cargo. And, the lessons we have learned will be applied throughout our entire port system. Simply put, Operation Safe Commerce -- and all of you -- have provided us a better way to protect our ports, our communities, and our economy."



Port of Karachi, Pakistan

RiskWatch was proud to be part of Operation Safe Commerce.

ABOUT RISKWATCH

RiskWatch creates and markets compelling and cost-effective security and compliance software programs for self-assessment against requirement and standards. RiskWatch solutions are used to self-assess, measure compliance, identify and assess threat levels, discover vulnerabilities, support a loss prevention program, and recommend mitigative safeguards by Return on Investment. RiskWatch customers include Fortune 1000 companies including Constellation Energy, Metris, AFLAC, Abbott Labs, Pfizer, AT&T, Verizon, Bearing Point, as well as federal and military clients including NSA, U.S. Department of Defense, U.S. Dept. of Veterans Affairs, University of Miami and many more.



1- 410-224-4773, x107
www.riskwatch.com