

Week 4

Screening cargo a mammoth duty

Companies get set for costly, time-consuming expansion of air security policy

By Thomas Frank
USA TODAY

DULLES, Va. — Tim Holdaway's job seems simple: send a truck to pick up shipments of computers and TVs from manufacturers and get the boxes to an airport.

Starting in the next year, Holdaway and companies like his, Cavalier Logistics, will take on a task that could change aviation security and international commerce.

In one of the biggest and costliest expansions of aviation security since 9/11, hundreds of companies such as Cavalier are gearing up to screen tens of millions of boxes of merchandise before those boxes are loaded onto U.S. passenger airplanes to be carried each year to retailers and others around the world.

Democrats in Congress ordered the screening last year as a way to stop terrorists from using a cargo shipment to blow up a passenger plane. Cargo is not required to be screened before it is loaded with luggage under a passenger cabin.

A 2007 law requires cargo on passenger planes to be screened. The system is being phased in. By 2010, all cargo on passenger



Brendan Hoffman for USA TODAY

The business of "airforwarding": Alejandro Najarro, right, uses a forklift to unload cargo from a truck with the help of driver Scott Evans at a Cavalier Logistics warehouse April 25.

planes must be screened. That could have far-reaching effects.

Congressional researchers estimate the screening equipment and personnel will cost \$3.75 billion over 10 years. Transportation expert Brandon Fried says screening could take so long that shipments would be delayed and "factories could shut down." Security consultant Douglas Laird questions whether companies that specialize in trucking freight can secure aviation. He calls the

entire process "folly."

"You're spending a lot of money for not achieving much," says Laird, former security chief at Northwest Airlines.

Working with airlines, manufacturers and transport companies, the Transportation Security Administration (TSA) is developing a system to do what was once thought impossible: screen more than 600,000 boxes of cargo a day for bombs.

Unlike the 2 million daily airline passengers and their 1.5 million pieces of luggage, cargo will not be screened by the TSA at airports. That's because cargo often arrives at airports packed in aluminum crates the size of a small car, and there isn't time to take apart the crates so each box holding one computer or TV set can be screened individually.

The TSA's solution: have the screening done by people who pack the crates. "We want the supply chain, before they assemble a load, to take individual boxes and screen them," TSA Assistant Administrator John Sammon says.

The middlemen

The plan puts the spotlight — and financial pressure — on companies such as Cavalier, which would buy and operate bomb-detection machines.

"From a cost standpoint, it's substantial," says Holdaway, Cavalier's president. He's standing in Cavalier's 60,000-square-foot warehouse near Washington Dulles International Airport as the beeping whine of a forklift echoes off the concrete floor.

Cavalier has 200 employees and seven warehouses — most near a major U.S. airport. It functions as a middleman for companies that want goods shipped long distances but don't want to arrange the transport. It's one of 4,000 "airforwarders" that handle 80% of cargo loaded on passenger planes.

Cavalier truck drivers bring merchandise to a warehouse. Laborers pack the boxes into big

containers. Booking agents line up flights to take cargo around the world. Truckers drive to an airport. "We warehouse, ship, consolidate and store," Holdaway says.

Laird wonders whether the new system can keep bombs off planes.

"When the screening is dispersed to so many locations, how are you going to ensure that the screeners at these facilities meet the same qualifications as the TSA screeners at airports?" Laird says. "Who's going to ensure that everything is done properly?"

Laird also questions whether a terrorist would plant a bomb in a cargo package because the package might end up in an all-cargo plane flown by a company such as FedEx.

Rep. Ed Markey, D-Mass., who led a four-year fight to require cargo screening, worries about how boxes that have been screened will remain secure while being driven to an airport.

Training and inspections

Sammon says screeners working for airforwarders will get similar training to TSA airport screeners and will be monitored by agency inspectors who'll make unannounced visits. The TSA is developing seals for screened boxes that would indicate tampering if broken. Sammon has signed up 20 airforwarders near major airports such as Chicago O'Hare to test a screening system in a few months.

Airforwarders will not be required to screen cargo they take to passenger planes. They are free to do no screening. Sammon says

many will do the screening because it will help business. Airlines will have to screen cargo they receive that has not been checked.

That could "cause massive bottlenecks, because airlines don't have the manpower, equipment or real estate" to do extensive screening, says Fried, executive director of the Airforwarders Association. "You're going to have backlogs and products that don't make it to market on time, or store shelves that go empty. Factories could shut down because they can't get inventory parts."

Michele Siano, compliance officer for Cavalier, says TSA officials have told her cargo packages might have to wait four days at an airport if her company does not screen them. "There is no option for us" but to screen packages, Siano says.

Week 4

Discussion

1. Why do you think the U.S. government hasn't required cargo to be screened before now?
2. What is the estimated cost of cargo screening equipment and personnel?
3. What is an "airforwarders" job?
4. There are multiple stops along a supply chain in which a shipment could be screened. List them.
5. When, along the supply chain, do you think it is most realistic or efficient for a shipment to be screened? Why?
6. List all of the challenges associated with screening tens of millions of boxes. Is screening tens of millions of boxes realistic?
7. Is screening cargo necessary for national security?

Activity

The physical supply chain described in the article is utterly dependent on the Internet. Every step along the way, from communication to shipment logistics, is planned, communicated and confirmed through various Internet-based systems. Just as the physical supply chain needs to be secure, so too does the Internet that it relies on. But just as screening tens of millions of boxes presents staggering challenges, so too does protecting the information infrastructure dependent on the Internet. In the grid below, the left column lists several aspects of a physical supply chain. In the right column, you and a partner should indicate what you think the cyber-equivalent of each aspect could be. As an example, the first one has been done for you. When you are finished, compare your grid with that of another set of partners. Did you come up with similar equivalents? Finally, as a group of four, answer the two questions below the grid.

Aspects of a physical supply chain	The cyber-equivalent of that physical aspect
Screening tens of millions of boxes	Virus software screening tens of millions of e-mails
Bombs in cargo	
Screening boxes before they are packed into cargo containers	
60,000-square-foot warehouse near the airport for storing shipments	
Trucks/planes for transporting goods	
"Airforwarders"	
Keeping boxes secure en route	
The Transportation Security Administration	

1. If cyberterrorists were able to shut down one of our essential supply chains (for example food) by attacking its Internet-dependent communication and logistics systems, what would the consequences be?
2. The article makes it clear that the U.S. government is getting serious about securing physical supply chains. List ways that it could begin securing the Internet-dependent infrastructure that our supply chains depend on.

Lesson objectives:

TEACHER'S GUIDE

In this lesson, students will:

- ▶ Read about securing U.S. supply chains.
- ▶ Identify the different aspects of a supply chain.
- ▶ Evaluate the challenges of screening tens of millions of boxes.
- ▶ Determine cyber-equivalents to aspects of a physical supply chain.
- ▶ Consider the repercussions of a cyberattack on a U.S. supply chain.
- ▶ Ascertain ways to safeguard against cyberattacks on U.S. supply chains.

Time requirements:

Step 1: Read the article (10 minutes).

Step 2: Answer the discussion questions (15 minutes).

Step 3: Complete the grid and answer the two analysis questions that follow it (20 minutes).

Step 4: Share responses to the two analysis questions as a class (10 minutes).

Total: 55 minutes

Recommendations:

Step 2: It is best to facilitate a whole class discussion to ensure student understanding of the concepts. You may wish to create a representation of a supply chain on the board so students understand the various aspects of it. You may also wish to list the answers to Questions 4 and 6 on the board.

Step 3: Before students get into pairs, you may wish to model the activity by having the class brainstorm a potential answer to the second row of the grid. Once students are in pairs or groups of four, circulate to ensure they are on task.

Step 4: To close the lesson, have groups share and debate their answers to the two questions that follow the grid.

Links:

- ▶ National Cyber Security Alliance: www.staysafeonline.org
- ▶ The Department of Homeland Security's Critical Infrastructure/Key Resources Protection Resources: www.dhs.gov/xprevprot/programs/editorial_0211.shtm
- ▶ Transportation Security Administration: www.tsa.gov
- ▶ Federal Trade Commission: www.onguardonline.gov
- ▶ United States Computer Emergency Readiness Team: www.us-cert.gov
- ▶ i-SAFE: www.i-safe.org
- ▶ Wired Safety Organization: www.wiredsafety.org
- ▶ Multi-State Information Sharing and Analysis Center: www.msisac.org/awareness

TEACHER'S GUIDE

Week 4

Industry association links:

- ▶ A public service website sponsored by Internet industry corporations and public interest organizations: www.getnetwise.org
- ▶ The Anti-Phishing Working Group (APWG): www.antiphishing.org
- ▶ Direct Marketing Association: www.the-dma.org/index.php
- ▶ The Sans Institute: www.sans.org
- ▶ The Computing Technology Industry Association: www.comptia.org