Customs-Trade Partnership Against Terrorism (C-TPAT)

Security Breach Preventive Measures Workshop

Bryant Van Buskirk, Supervisor
Los Angeles C-TPAT Field Office

Osvaldo Martin, Supervisor
Houston C-TPAT Field Office

Arthur Qureishi, C-TPAT Program Officer
Washington, DC
Security Threats

“Cargo is vulnerable when procedures break down, rules are not followed and errors are made. Sound management is needed to forge the chain that will link together all the parts of an operational security system.”
Roles & Responsibilities…

C-TPAT

- Maintain and evaluate the minimum security criteria
- Certify, Validate and Revalidate member supply chains

Participants

- Continued commitment to the program
- Annual self-assessment to include:
  - Verification of supply chain security processes
  - Self-policing or Auditing to ensure compliance
C-TPAT Minimum Security Criteria

- The starting point for making effective security practices.

- Incorporating the criteria into your business can improve the performance of your business and will lessen the chances of a security breach.

- Strong supply chain security measures reduce the risk of loss, theft, and smuggling.
C-TPAT Minimum Security Criteria

- The supply chain for C-TPAT purposes is defined from point of origin (manufacturer/supplier/vendor) through to point of distribution.

- CBP is concerned about security of the container as it travels through the supply chain and clears final CBP processing at the Port of entry.

- Once it clears CBP, the importer and others still have a role to ensure that cargo is not compromised prior to reaching final destination.
Security Breach Defined:

Introduction of the following into the supply chain:

- Prohibited or otherwise illegal products, substances, or people

Deliberate or unintentional introduction of products that are:

- In violation of a Government’s laws and regulations
Common Factors/Observations

Breaches are breakdowns or failures involving security measures for:

- People
- Processes
- Technology – (Equipment/Information)
Common Factors/Observations

People

- Personnel Security (Internal Conspiracy)
  - Failure to conduct checks/re-checks
  - Failure to identify change in employee behavior
Common Factors/Observations

People

- Training & Awareness
  - Employees not trained to identify problems/anomalies
  - Employees not encouraged to communicate problems to management
  - No incentives for employees to actively participate in company security program (not necessarily monetary)
Common Factors/Observations

Processes

- Risk assessment of supply chain not conducted or incomplete
- No written policies/procedures
- Outdated policies/procedures
Common Factors/Observations

Processes

- Failure of employees/management to follow established policies & procedures/not trained properly

- Security measures never tested/audited

- Change in business partners – security not assessed
Common Factors/Observations

Processes

- Lack of checks, balances, accountability/responsibility

- Unaware of sub-contracting of products & services in the supply chain to “other” business partners

- Change in supply chain used (Cargo Flow/Trade Lane)
Common Factors/Observations

Technology/Equipment/Information

- Failure to control and monitor access to/track instruments of international trade and transportation

- Equipment is faulty – e.g. latches on containers/trailers inadequate, surveillance cameras/monitoring system not working

- Technology not kept up-to-date with growth/size of company – e.g. access controls
Common Factors/Observations

Technology/Equipment/Information

- Uncontrolled access to equipment and technology used for surveillance and monitoring the facility
- Uncontrolled access to information: automated or paper – shipping, receiving & financial information
Patterns of risk enabling security breakdowns:

- Management doesn’t ensure that employees are following their own security procedures.

- The company and employees are not aware of the risks they encourage by having poor security practices.

- Pattern of pushing responsibility for security to the ‘other’ C-TPAT member(s).
Policies and Procedures...

Inspection processes should be in place at all locations:

- Manufacturers
- Suppliers
- Vendors
- Logistical Service Providers
- Distribution Centers
- Container Storage Depots
- Warehouses
Subcontracting/Monitoring...

Security breach involving shipments of produce
Conveyance Security…

Security breach as a result of not monitoring transit times
Trailer Storage and Inspection...
Business Partner Selection...
Business Partner Selection…

A new feeder service…
Container Storage/Security …
Similar delivery systems

The Alfred P. Murrah Federal Building before truck bombing

After truck bomb
## Identifying Issues – 6 Questions

<table>
<thead>
<tr>
<th>Question</th>
<th>How Applies to Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who?</td>
<td>Accountability</td>
</tr>
<tr>
<td>What?</td>
<td>Object</td>
</tr>
<tr>
<td>When?</td>
<td>Timing</td>
</tr>
<tr>
<td>Where?</td>
<td>Location</td>
</tr>
<tr>
<td>How?</td>
<td>Procedure/Method</td>
</tr>
<tr>
<td>Why?</td>
<td>Purpose</td>
</tr>
</tbody>
</table>
C-TPAT Minimum Security Criteria

It is the responsibility of the member to study their supply chain(s), assess the risk, and then develop security controls to deal with those risks.

Identify the dangers or vulnerabilities to your business that you should avoid.
Analyzing Security Breaches

Group Exercise

- View the image.
- Think of how the trailer or product was compromised.
- Where do you think the security breakdown occurred?
- What C-TPAT Security Criteria/Guideline was not followed?
- How do you prevent this from happening to your business?
Empty Truck Trailer

Do you have any concerns about the appearance of this empty container?
Empty Trailer – False Wall

What areas in the C-TPAT criteria may have been compromised?
Modified Trailer

Container Inspections

Container Storage

Training and Security
Awareness

Monitoring/Tracking

Personnel Security

Business Partners

Homeland Security
Cargo Container

Do you have any concerns about the appearance of this container?
Cargo Container – Floor Modification
Modified Container

Container Inspections

Container Tracking & Monitoring

Security Training and Awareness

Container Storage

Business Partners
New Customer
Risk to your Business

Business Partner Selection

Customer Screening Processes

Security Training and Awareness

Request for Inspection?
Almost All Cargo Can Be Compromised
Most common areas of failed criteria:

- Conveyance Security – Tracking & Monitoring 51%
- Container Security – Sealing/Container Inspections 49%
- Business Partners – Screening & Subcontracting 46%
- Personnel Security – Background Checks 31%
Trend Analysis

Contributing Factors:

- Internal Conspiracy: 74%
- Threat/Intimidation: 3%
- Bribes: 11%
- Unspecified: 12%
Trend Analysis

Location of Compromise:

- In transit: 51%
- Factory: 25%
- Exchange Hub: 17%
- Unspecified/Other: 7%
Trend Analysis

- Procedures in Place at time of Security Breach:
  - 51% Yes
  - 49% No

- Were Procedures Followed?
  - 17% Yes
  - **83% No**
Best Practices

- Company conveyances are tracked and monitored utilizing a global positioning system (GPS) technology.

- GPS tracking device provides real-time status of conveyances from the time of departure at the storage yard to the loading point at the shipper’s facility, while en route to the U.S. border, and to delivery destinations.

- The GPS tracking system also identifies predetermined routes for drivers to utilize. Any deviation from these routes alerts company management.
Best Practices

- GPS signal return or ‘Ping’ rates are set at 10 – 15 minute intervals.

- At point of destination, arrival time, and verification of driver, trailer, cab and seal number is sent back to the manufacturer and highway carrier management.

- Highway Carrier uses GPS in conjunction with remote locking devices and remote engine kill switch.
Best Practices

- The conveyance can be remotely locked so that the driver no longer can access the conveyance.

- If a shipment/tractor is suspect or compromised, the truck can be disabled remotely.

- The company has preplanned check points identified if a truck needs to be disabled for inspection.

- Procedures are in place for a traffic management team to respond.
Best Practices

- Routes from the pick-up point to the destination are pre-designated.

- Drivers are provided just enough fuel to transport their shipments from point of origin to destination.

- All transit time is closely monitored.

- All shipments are direct delivery - Drivers are not allowed to stop enroute.
Best Practices

- Trucks and trailers are inspected prior to crossing the Border. This provides an additional layer of conveyance, commodity, and seal verification prior to the shipments arriving in the United States.

- Management photographs the residences of all drivers yearly to check that drivers are not living beyond their means.

- Truck dispatch staff is routinely rotated on an unannounced basis.
Best Practices

- At unannounced and intermittent intervals, company management will follow loaded trailers from point of origin until crossing the border into the US, documenting driver adherence to company’s transportation policy.

- Dispatch logs are recorded electronically.

- The company will not use any border-crossing highway carriers that are not C-TPAT and/or FAST certified.
Best Practices

- The cargo loading process is digitally recorded. Photographs are taken of the loading of each shipment, documenting the integrity of the cargo. Images include photographs showing the placement of palletized cargo, invoice, tractor and trailer plates, trailer number and seal.

- Digital pictures are sent back to the manufacturer upon arriving at destination.
Best Practices

- Company uses both a High Security Bolt seal and a High Security Cable seal to secure all shipments.

- Company utilizes a unique PAS ISO 17712 high security seal that changes bolt color if altered and/or cut.

- The company conducts quarterly self assessments in conjunction with annual assessment to ensure the company’s security practices are in place and working.
Best Practices

- Quarterly business partner and customer/client audits are also performed using a score card system, while broker audits are conducted annually.

- C-TPAT members should never allow their import identification numbers to be utilized outside of any business they don’t exercise direct and full control over - SCAC codes, Manufacturer IDs, IOR numbers.
Seals and Door Hardware
Seals and Door Hardware
Seals and Door Hardware

Seals should be affixed to the right door on the hasp that has the welded rivets.
Seals and Door Hardware
Security Breach Demo
Seals and Door Hardware

Seal stem is bent. Seal does not lock properly.
Seals and Door Hardware
Seals and Door Hardware
Conveyance Security & Sealing
Conveyance Security & Sealing
In-House Repairs
Door Hardware & Fasteners

Left side rear door, bottom bolts
Door Hardware & Fasteners
How to Report Suspicious Activity

- 1-800-BE-ALERT
- Don’t settle for voicemail
- CBP Website:
  www.cbp.gov/xp/cgov/toolbox/contacts/ports
How to Report Suspicious Activity

Report Suspicious Activity to 1-800-BE-ALERT
How to Report Suspicious Activity

Ports of entry are responsible for daily port specific operations. There are 327 official ports of entry in the United States and 15 Preclearance offices in Canada and the Caribbean. Port personnel are the face at the border for most cargo and visitors entering the United States. Here CBP enforces the import and export laws and regulations of the U.S. federal government and conducts immigration policy and programs. Ports also perform agriculture inspections to protect the USA from potential carriers of animal and plant pests or diseases that could cause
How to Report Suspicious Activity

Service Port-Los Angeles/Long Beach Seaport

Port Information
- Port Code: 2704
- Location Address: 301 E. Ocean Blvd,
  Suite 1400
  Long Beach, CA 90802
- Mailing Address: Same As Above
- General Phone: (562) 366-5555
- General Fax: (562) 628-7900
- Operational Hours: 8:00 AM-4:30 PM(Pacific)
  Weekdays (Monday-Friday)
- Description: A Service Port is a CBP location that
  has a full range of cargo processing functions, including inspections,
  entry, collections, and verification (19 CFR 101.1).
  Brokers: View List

Service Contacts
- Name: Broker Management Office
- Phone: (562) 366-5404
- Fax: (562) 628-7906

see also:
- In California:
  - Andrade - Class A
  - Caldecote East - Class A - (Service Port)
  - Caldecote West - Class A
  - Eureka
  - Fresno (2003/2002)
  - Port Hueneme
  - ...more

On CBP.gov
- Border Wait Times
- Questions
- Pleasure Boats
How to Report Suspicious Activity

C-TPAT
- Your assigned Supply Chain Security Specialist
- C-TPAT Field Offices:
  - Buffalo 716-626-6470
  - Houston 713-744-8020
  - Los Angeles 562-366-3280
  - Miami 305-471-8080
  - Newark 908-353-6818
  - New York 718-553-2745