

# C-TPAT Supply Chain Security Panel

March 18, 2010

## Tools, Technologies and Processes: Innovative Industry Solutions to Security Challenges

Barry Brandman  
President/CEO  
Danbee Investigations

# Evaluating the True Effectiveness of a Supply Chain Security Program

## *3 Realities*

### “Separating Fact From Fiction”

Most security programs look much better on paper than they are in reality

The difference between a vulnerable supply chain security program that relies on cosmetic controls and an effective program composed of meaningful safeguards, is seldom obvious

Exposing your weaknesses before they can be exploited is of critical importance. Those companies that have failed to do so have been victimized far more frequently than those that proactively uncover and correct their deficiencies

## Example of Issues Exposed During International Security Audits

- False sense of security, which oftentimes breeds complacency
  - ┌ *Example: “C-TPAT Certified” foreign freight forwarder*
- Lack of available expertise in many countries for the design and programming of state of the art security technology
  - ┌ *Example: Export department was not properly protected with intrusion detection and video systems during times that it was not in operation and U.S. imports were vulnerable*

# Example of Issues Exposed During International Security Audits

- 7-Point inspection failures
  - ┌ *Example: Inadequate understanding of how to perform inspection*
  - ┌ *Example: Leaving partially loaded containers exposed during breaks and shift changes*

# Inherent Weaknesses With The Design Of Most Intrusion Detection Systems

1. Relying on vendor sales representatives to design electronic protection:
  - These personnel are rarely educated on how their systems have been defeated. Their focus is marketing, not forensics.
  - Vendors have no financial responsibility for loss that subsequently occurs
2. Not restricting access to the head-end room by employees, vendors, and contractors
3. Not having the head-end room electronically protected from internal and external attack

## Inherent Weaknesses With The Design Of Most Intrusion Detection Systems (cont'd)

4. Inadequate backup communication with the central station monitoring the system
5. Failing to control bypass capability
6. Not having electronic supervision of all the system's components
7. Using the wrong type of interior traps to supplement magnetic door contacts
8. Having technicians neutralize motion detectors during service calls
9. Failing to conduct a complete system-wide testing at least once per year

# Inherent Weaknesses With The Design Of Most Video Systems

1. Not programming the DVR/NVR to record on motion-based activity
2. Sacrificing recording quality because of a hard drive that is inadequate
3. Not having notification of failure to operate/record
4. An over-reliance on pan/tilt/zoom cameras
5. Using cameras that do not have the capability to compensate for extremes in ambient lighting

## Inherent Weaknesses With The Design Of Most Video Systems (cont'd)

6. Designing video coverage of dock/loading areas that:
  - a. Can't definitively "recreate reality" of freight movement
  - b. Doesn't show seals being affixed/detached
  - c. Doesn't show the inspection process of empty containers/trailers
7. Not using the video system proactively
8. Not having the complete chain of custody video coverage (assembly line, staging area, path to the shipping department, stretch wrap machine, staging area and shipping dock/truck) at foreign facilities

# A MAJOR SECURITY CHALLENGE IN CERTAIN FOREIGN COUNTRIES

## **CORRUPTION IN THE SECURITY INDUSTRY**

- Guard companies are oftentimes part of the problem rather than solution:
  - Unregistered personnel
  - Inadequate screening policies
  - Invoicing for phantom hours of coverage
  - Poor compensation results in frequent turnover and high risk for bribery
- Yet for many companies guards are oftentimes the primary safeguard used in foreign countries. If the guards are not trustworthy, the integrity of the supply chain can be easily compromised.

# SEAL CONTROLS

A CRITICAL COMPONENT OF EVERY  
SUPPLY CHAIN SECURITY PROGRAM

What Are Effective Security  
Practices That Will Provide Chain  
of Custody Integrity?

# Security Seal Best Practices

1. Notify the security seal manufacturer to only accept an order and ship to a designated company representative at an authorized address
2. Upon arrival, wrap the boxes waiting to be used with tamper-evident security tape and store in a secured area with controlled access
3. Ration seals as needed on a daily basis and keep loose seals in a secured location rather than exposed

## Security Seal Best Practices (cont'd)

4. Restrict seal handling responsibilities only to authorized personnel
5. Distribute and use seals in numerical sequence and conduct reconciliations on a daily basis
6. The entire seal process should be under continuous viewing and archiving by your video system so the established chain of custody procedures can be proactively audited and available for post incident investigations

# GPS Best Practices

1. Don't assume that programming was done correctly and is operating properly
2. Static geo-fencing is helpful, but not a truly effective security control
3. A system with exception reporting (violation authorized routes, excessive stop times, signal loss, etc.) is always preferred

## GPS Best Practices (cont'd)

4. Verify that reports are being reviewed by authorized security personnel, in addition to dispatch staff, or utilize a redundant monitoring station
5. With trucks transporting imports from Mexico, special procedures should be established when seals are removed and the cargo area is opened by Mexican military or police
6. Test the competency of monitoring personnel with unannounced simulated security breaches

**“Never confuse being good with being lucky”**

**C-TPAT Supply Chain Security Panel**

**March 18, 2010**

**Tools, Technologies and Processes:  
Innovative Industry Solutions to Security  
Challenges**

**Barry Brandman**

**President/CEO**

**Danbee Investigations**

**[bbrandman@danbeeinvestigations.com](mailto:bbrandman@danbeeinvestigations.com)**