Security Breaches & Internal Conspiracies

U.S. Customs and Border Protection

Workshop Objectives

- Internal Conspiracy Case Studies
- Effective Preventive Measures
- Internal Conspiracies Defined
- Internal Conspiracy Indicators
- Best Practices

Case Study #1

- Information received that drug trafficking organization (DTO) has built hidden compartments within the structures of multiple trailers to smuggle narcotics across the Canadian/ United States border.
- Trailers are loaded with narcotics prior to arriving at foreign manufacturer/ consolidator facility.
- Trailer inspections are conducted, cargo is loaded and a high security seal is affixed to the trailer door.
- Trailer shipments are monitored by the transport company via GPS and cell phone communication with the drivers.

Case Study #1

U.S. Customs and Border Protection

Case Study #1

- Possible conspirators:
  - Transport company/ employee
  - Driver
  - Foreign manufacturer/ consolidator employee(s)
  - All of the above
- What preventive measures can a company implement to minimize this type of security breach?

Preventive Measures

- Conduct a comprehensive risk assessment of the company's international supply chain. Based upon a documented risk assessment process, non-C-TPAT business partners must be subject to verification of compliance with security criteria.
- Conduct on-site visits of service providers' facilities to verify security measures.
- For those business partners eligible for C-TPAT certification the company must have documentation indicating whether these service providers are or are not C-TPAT certified (monitor SVI number, AEO certificate, ISO 28000, etc.).
- Request drivers that have been issued a Free and Secure Trade (FAST) licenses. These drivers go through additional scrutiny by CBP.

Case Study #2

- Container/ trailer locking mechanisms are attacked prior to arriving at foreign manufacturer facility.
- Container/ trailer inspections are conducted and documented at export warehouse.
- A high security seal is affixed to the container/ trailer door by an authorized company employee.
- Upon exiting the facility, shipment documents and affixed seal are verified by a security guard at the main gate.
- Container/ trailer shipments are tracked by the carrier via on-line website, GPS and cell phone communication with the drivers.

Case Study #2

U.S. Customs and Border Protection

Case Study #2

- Possible conspirators:
  - Driver
  - Foreign manufacturer employee conducting container/ trailer inspections
  - Security guard(s)
  - All of the above
- What preventive measures can a company implement to minimize this type of security breach?

Preventive Measures

- Obligate carriers to provide containers/ trailers that have been inspected (7-point container inspection) and are free from security vulnerabilities.
- Conduct on-site visits of carriers' facilities to verify how container/ trailer inspections are conducted.
- Provide container/ trailer inspection training to specific individuals throughout the company's supply chain. (carrier, warehouse employees, security guards, etc.)
- Confirm hiring practices of security company providing guards. Make sure hiring practices are in line with foreign manufacturer requirements.
- Verify how container/ trailers are tracked by carriers' monitoring systems. Are notification alerts active. (on-line tracking, e-mails, GPS, Geo-fencing, etc.)

Internal Conspiracies

- Supply chain security is the responsibility of all C-TPAT certified companies from point of origin through point of distribution.
- Look at the entire supply chain as one security system NOT segmented with different layers of responsibility.
- Establish checks and balances.
- Verify all business partners and conduct documented on-site security verifications.
- Demand contractual obligations regarding established security practices.
- How can security vulnerabilities/ deficiencies be found if they are not being searched for?

Internal Conspiracies

- Definition - when **people** work **together** by agreeing to commit a crime, fraud, or other wrongful act. A conspiracy may exist when the parties use legal means to accomplish an illegal result, or to use illegal means to achieve something that is unlawful.
- Money is the main motivator for the internal conspirator. For relatively "easy" work (removal, delivery, lookout) the reward is substantial.

U.S. Customs and Border Protection

Internal Conspiracies

Average price of illegal narcotics:

- Marijuana - $500 to $1,000 per pound

  (Canadian marijuana can be 300%-600% more expensive)
- Cocaine - $15,000 to $21,000 per kilo
- Heroin - $30,000 to $40,000 per kilo
- Transportation costs, drug purity & risk of being captured are some factors that are calculated into the price.
- Global revenue from illegal drug market: **300 - 350 billion**
- Proceeds of illegal drug trafficking are used to fund additional criminal acts like terrorism, purchases of unauthorized weapons/ ammo & human smuggling.

Internal Conspiracies

- Terrorists may use the same techniques that narcotic smugglers use or hire a DTO to smuggle for them!!!
- Risk of capture may be minimal due to:
  - High volume of container traffic not inspected/ scrutinized by Law Enforcement (lack of manpower).
  - Corrupted security personnel throughout the supply chain. Lookout – "I didn't see or know nothing"
  - Company/ employees threatened and afraid of retaliation.
- Internal conspiracy is the cheapest and easiest method when attempting illicit activities….plenty of $$$ to go around.
- For legitimate businesses – imported goods and containers/ trailers are currently used as conveyances to smuggle contraband with the result being financial loss and bad publicity for the company.

Internal Conspiracies

The eight signs of terrorism:

1 - Surveillance

2 - Information Gathering

3 - Tests of Security

4 - Funding

5 - Acquiring Supplies

6 - People who don't belong

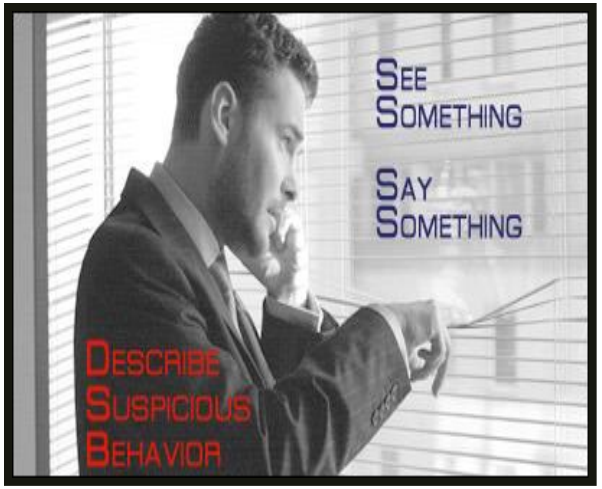
7 - Trial Run

8 - Deploying Assets

U.S. Customs and Border Protection

Conspiracy Indicators

- Conspirators will conduct surveillance and gather information about the facility's operations and security protocols.
- May take photographs and/or videos of the facility's physical security to include entrances, fencing, buildings, light poles and CCTV camera locations.
- Conspirators will TEST the company's security system to evaluate reaction or non-reaction times.



U.S. Customs and Border Protection

Conspiracy Indicators

- Internal conspirators will seek out information about the company's security procedures. May use social engineering tools to gather information about the company and employees.
- Will ask questions on how shipment routes are monitored, GPS system works, document routing, manifests, etc.
- Cargo transit routes and stops are of particular interest.
- Access to stow plans of containerized cargo will allow for quick and easy access to introduce illegal contraband.
- Gather information on employee schedules, work habits, lunch breaks, off-duty social life, home address, etc.
- By assessing the company's probable vulnerabilities the conspirator can determine a good opportunity for the breach to occur.

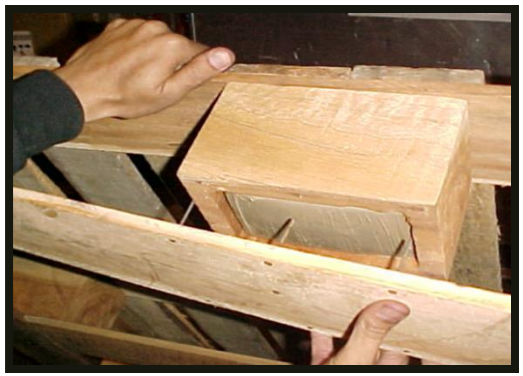
Conspiracy Indicators

Probe the company's security (Trial Run):

- May show up to work on day off
- Enter restricted and/or unauthorized areas without proper access/identification
- Enter the shipping warehouse with unauthorized personal items (backpacks, laptops, smart phones, etc.)
- Activate alarms and check for reaction time
- Change work schedule to evaluate security at another time
- May ship an un-related item with legitimate cargo
- Entering false information in the documents such as a bogus address, name, "fictitious" company, etc.
- Attempting to pick-up cargo without appropriate documentation and identification
- Drivers may stray off the authorized route to test GPS geo-fencing
- Planned delays during transport to **TIME** the company's response
- Unique markings/ tape on legitimate cargo boxes/ pallets

Conspiracy Indicators

- Acquiring company equipment:
  - Company uniforms, identification, access cards, keys & alarm codes to enter sensitive areas
  - Report company items lost or stolen in order to duplicate
  - Stolen high-security seals and/ or disposed cut seals
  - Obtaining company boxes/ crates/ pallets conceal the contraband
- All company personnel (not only security guards) should be on the lookout for suspicious people/ activity occurring around the facility!!!
- Train company employees to challenge and report unauthorized individuals to management/ security personnel.



U.S. Customs and Border Protection

Best Practices

- Reporting suspicious activities for employees:
  - Phone numbers posted throughout facility (security guards, supervisors, local law enforcement, etc.)
  - Awareness posters on what to do and who to contact
  - Anonymous Hotline
  - Incentives (recognition, award, monetary, etc.)
- Reporting supply chain security incidents for company:
  - Establish a reporting “calling tree”
  - Company corporate security department
  - Foreign government agencies/ law enforcement
  - CBP at Ports of Entry (POE) http://www.cbp.gov/contact/ports
  - C-TPAT/ Supply Chain Security Specialist (**important**)

Best Practices

- Conduct tests of security protocols - facility/ supply chain:
  - Access sensitive areas to see if confronted
  - Set off alarms and check for response time
  - Place suspicious backpack/ package inside facility to see if it is reported.
  - Turn off CCTV cameras and exterior lights to see if they are appropriately reported for repair.
  - Create incorrect shipping documents (packing list, bill of lading, etc.) and see if they are questioned prior to loading.
  - Apply wrong seal on container/ trailer and see if security guard verifies the seal number for accuracy before exiting the facility.
  - Escort shipment after exiting & see where it goes.

Best Practices

- Create a supply chain security team:
  - Meet with local law enforcement entities
  - Work with other companies in the same area/ industry
  - Periodic meetings to discuss security issues facing the company & possible improvements that can be made.
- Perform in-depth background checks for new employees to include social economic reviews. Periodic background checks should be conducted for vested employees especially if there is a change in duties or for cause.
- Establish property checklist for company items that are issued to employees upon being hired. Items like access badges, keys, uniforms, laptops & credit cards should be listed on the checklist. The checklist should be used to collect all items when the employee leaves the company.
- **TRAINING** (what to look for, challenging, reporting, etc.)

Summary

- Internal conspiracies are real & can happen at your company
- Financial gain is the main motivator for internal conspirators
- Establish robust security protocols (preventive measures) to minimize internal conspiracies/ security breaches at facility.
- Train company personnel to look for and properly report internal conspiracy indicators/ eight signs of terrorism.
- Regularly test security system(s) and establish corrective actions for vulnerabilities that are found.
- Incorporate security best practices throughout company's supply chain.

U.S. Customs and Border Protection