Protecting Your Company's Identity

Balancing Supply Chain Security and Economic Efficiency

Stages of Identity Theft

- **Acquisition of the identity** such as theft, internet, garbage and mail

- **Use of the identity** For financial gain (most common) and/or evade Law Enforcement

- **Discovery of the theft** Identity theft may take from six months to several years to discover. Evidence suggests the longer it takes to discover the theft, the greater the loss incurred by the victim.

Source: National Institute of Justice / U.S. Department of Justice

Acquisition

- “Dumpster diving” – going through garbage cans, dumpsters, trash bins to obtain copies of your documents that typically bear your name, address, and even telephone number. These types of records make it easy for criminals to obtain accounts in your name.
- “Shoulder surfing” – watching from a nearby location as you enter data into the computer or read trade sensitive information on your desk.
- Criminals buy old/unwanted computers and troll their hard drives for sensitive information. The same goes for Blackberries, Palm Pilots, and PDA’s, which often hold both personal and business-related information.
- “Insider” – employee steals sensitive data by removing paper documents or accessing electronic data. Criminals may bribe employees to gain access to sensitive company data.

Use / Discovery

- Confessed to stealing between one to two million dollars in cash and merchandise. All he needed to do was **find processed deposit slips and junk mail with full names and addresses in the garbage** of a local bank.
- Stole social security numbers and racked up $60,000 on credit cards. Police say she went looking for moving boxes, and **found the employment applications in the dumpster**.
- Cleaning worker arrested: **pulled papers from the trash barrel or recycle bin**… anything that had a name or Social Security number. She stated "**she had the codes to the offices**."
- Arrested for stealing one million credit card numbers: It started with accomplices driving around the city with laptops **looking for unsecured computer networks.**

Mitigate Risk

- Corporate identity theft is on the rise
- Use Minimum Security Criteria as a tool
- Contractually obligate business partners to adhere to MSC
  - Business Partner Requirements
  - Personnel Security
  - Procedural Security
  - Information Technology Security

❖ Reduce opportunities for criminals to obtain your information

Business Partner Requirements

- **Security procedures**
  For those business partners eligible for C-TPAT certification (carriers, ports, terminals, brokers, consolidators, etc.) the importer must have documentation (e.g., C-TPAT certificate, SVI number, etc.) indicating whether these business partners are or are not C-TPAT certified.
  For those business partners not eligible for C-TPAT certification, importers must require their business partners to demonstrate that they are meeting C-TPAT security criteria via written/electronic confirmation (e.g., contractual obligations; via a letter from a senior business partner officer attesting to compliance; a written statement from the business partner demonstrating their compliance with C-TPAT security criteria or an equivalent WCO accredited security program administered by a foreign customs authority; or, by providing a completed importer security questionnaire). Based upon a documented risk assessment process, non-C-TPAT eligible business partners must be subject to verification of compliance with C-TPAT security criteria by the importer.

***ASK*: How have we confirmed that our business partners meet MSC requirements?**

Business Partner Requirements

- Brokers must have written and verifiable processes for the screening of new business partners, beyond financial soundness issues, to include security indicators.
- Written procedures must exist to address the specific factors or practices as determined by CBP as sufficient to trigger additional scrutiny of the import transaction as informed by U.S. Customs and Border Protection (CBP).

- ***ASK*: What do we know about this business partner?**
  - Never met customer
  - Only contacts by fax, email or cell phone

- ***ASK*: Do we verify that the POA is legitimate?**

Personnel Security

- Written and verifiable processes must be in place to screen prospective employees and to periodically check current employees.
- **Pre-Employment Verification**
  Application information, such as employment history and references must be verified prior to employment.
- **Background Checks/Investigations**
  Consistent with foreign, federal, state, and local regulations, background checks and investigations should be conducted for prospective employees. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.
- **Personnel Termination Procedures**
  Companies must have procedures in place to remove identification, facility, and system access for terminated employees.

ASK: What do we know about the individuals that work in our facility?

ASK: Has all facility access been removed for separated employees?

Procedural Security: Documentation Processing

- Documentation Processing:
  Procedures must be in place to ensure that all information used in the clearing of merchandise/cargo, is legible, complete, accurate, and protected against the exchange, loss or introduction of erroneous information.
- ***ASK: How is trade sensitive documentation destroyed?***
  - Internal
  - Business Partners
- ***ASK: Did we revoke inactive POAs?***

Procedural Security: Documentation Processing

- Brokers must have procedures must be in place to ensure that all information provided by the importer/exporter, freight forwarder, etc., and used in the clearing of merchandise/cargo, is legible and protected against the exchange, loss or introduction of erroneous information.
- Review of documentation for completeness and clarity and contacting the business partner or importer/exporter, as necessary, to obtain corrected documentation or information.
- To the extent such information comes to the broker's attention, alerting the importer/exporter of its obligation to notify CBP and/or any other appropriate law enforcement agency of any errors and/or shortages and overages of merchandise that create a security risk in the supply chain, and providing assistance that is consistent with its for hire services in making such notification and correction of data as may be required or requested by the importer/exporter.

Procedural Security: Document Review

- Transportation Carrier personnel should be trained to review manifests and other documents in order to identify or recognize suspicious cargo shipments that:
- Originate from or are destined to unusual locations
- Paid by cash or a certified check
- Have unusual routing methods
- Exhibit unusual shipping/receiving practices
- Provide vague, generalized or poor information
- All instances of a suspicious cargo shipment should be reported immediately to the nearest CBP port of entry.

Information Technology Security

- Documentation control must include safeguarding computer access and information
- **Password Protection**
  Automated systems must use individually assigned accounts that require a periodic change of password.
- **Accountability**
  A system must be in place to identify the abuse of IT including improper access, tampering or the altering of business data. All system violators must be subject to appropriate disciplinary actions for abuse.

- ***ASK: Do only those with a "Need to Know" have access to sensitive information?***
  - Levels of access
  - Password protected
  - Anti-intrusion software

Monitor Your "Credit Report"

- ACE Reports to monitor import activity by IOR
  - Port, HTS, filer code, export countries

- Notify CBP when suspicious activity is identified
  - C-TPAT POC
  - Account Manager
  - Port

- Have all of the particulars available
  - Date
  - Entry Number / Bill of lading
  - How suspicious activity differs from normal import operations

➢ **Obtain an ACE Account Today – Type keyword "ACE Application" in search box on www.cbp.gov**

Be Proactive

- **Employees must be trained to report suspicious activity**

- **Verification** of Power of Attorney
  - Do you know the customer?
  - Do you know the individual named on the POA?
  - Confirm that customer is legitimate
  - Contact company to verify POA

- Who has **access** to company information?
  - Is sensitive information secure after business hours?
  - Cleaning crew: do you know who they are?
  - Other employees without a “Need to Know”
  - IT disabled after employee separates from company

- **Disposal** of trade sensitive information
  - Paper documents: shred, burn bag, etc.
  - Wipe all files off old computers and PDA’s before getting rid of them. Hackers buy such devices for the information stored on them.

Case Study

2010

Balancing Supply Chain Security and Economic Efficiency