Risk Assessments and Risk Based Supply Chain Security

March, 2010
Risk Based Supply Chain Security

- What is Risk?
- What a Risk Assessment Isn’t
- What a Risk Assessment Is
- How does the Risk Assessment fit into the C-TPAT program?
- How can our company do an International Supply Chain Security Risk Assessment?
- How do the C-TPAT standards fit into a Risk Based Supply Chain Security Program?
- How can I develop a Risk Based Action Plan for Supply Chain Security?
Risk Based Supply Chain Security

What is Risk?

The determination of a potential adverse outcome that is a function of an agreed upon rule to measure/assess the likelihood of occurrence (threats), vulnerabilities and consequences associated with an incident, event or occurrence.
Risk Based Supply Chain Security

What a Risk Assessment Isn’t:

- Not just a Threat Assessment (e.g. Anything out of Mexico is high risk because of the cartels)
- Not just a Vulnerability Assessment (e.g. That is a high risk site, they don’t have any good security measures in place)
- Not just a Consequence Assessment (e.g. That’s high risk electronics cargo…but it’s insured)
- Not just using intuition (e.g. I’m a security professional and I know ‘high risk’ when I see it!)
Risk Based Supply Chain Security

What is a Risk Assessment?

- As we have learned, sometimes the term is misused even by security professionals
- DHS, DoD, state and local governments – same approach
- ISO 28000 (Supply Chain Security) – same approach
- British CRAMM, French Marion – same approach
- All share a common process model, even if precise terms vary slightly…and that is:
Risk Based Supply Chain Security

Determining Risk is a qualitative/quantitative process of combining the evaluated…

• **Threats** (likelihood of occurrence)

• **Vulnerabilities** (weaknesses or gaps in security from established standards; a measure of security effectiveness)

• **Consequences** (impact of adverse occurrences)
Risk Based Supply Chain Security

Threat Assessment:

A holistic assessment of all Threats to the international supply chain:

- Terrorism
- Contraband (e.g. illegal drugs)
- Illegal weapons
- Human smuggling, stowaways
- Disease
- Fire/Explosion
- Economic conditions
- Natural disasters
- Political unrest
- Labor problems
- Industrial espionage
- Organized crime
- Theft
- Product tampering
- Illegal currency

Questions: Is this threat relevant for this location? How did we make that decision? Based on what quantitative evidence?

*Remember…the Threat is constantly evolving and changing*
How can my company conduct a Threat Assessment?

• The more holistic, the more accurate for dealing with all issues
• Can be complex and address a variety of issues including historical record, capabilities, tactics, etc.
• Can involve complex matrices and scatter diagrams, etc.
• As a minimum focus on supply chain related issues
  – Terrorism
  – Cargo Theft
  – Hijacking
  – Drug smuggling
  – Port Security
  – IP/Brand Protection
  – Your security records
• Use contract services who have experts on-the-ground, use commercial security reporting services such as IJet or CAPRisk (these may not cover your areas of concern)
• Use government resources such as the Overseas Security Advisory Councils (OSAC), contact the Legal Attaché or Resident Security Officer in the Embassy, if out of the U.S., and CBP too; local police
• Professional association such as ASIS International, TAPA, etc.
• Determine an overall Threat rating (e.g. high, medium, low, etc.)
• Assign a value to that rating
Risk Based Supply Chain Security

CBP can help you with data such as:

• Most Common Areas of Failed Criteria:
  – Conveyance Security (tracking and monitoring) ............... 51%
  – Container Security (seals and inspections) .................. 49%
  – Business Partners (screening and subcontracting) .......... 46%
  – Personnel Security (background investigations) ............ 31%

• Location of Compromise:
  – In transit ................................................................. 51%
  – Factory ................................................................. 25%
  – Exchange Hub ....................................................... 17%
  – Other ................................................................. 7%
Risk Based Supply Chain Security

Vulnerability Assessment:

An assessment of existing gaps and exploitable weaknesses (Vulnerabilities) from established security standards at all points in the flow of cargo within the international supply chain:

- Business Partner Requirements
- Securing the instruments of traffic or conveyances (e.g. container/trailer security)
- Access Controls
- Personnel Security
- Procedural Security
- Physical Security
- Information Technology Security
- Security Training and Threat Awareness

Question: Does the facility meet the standards or not? Evaluate each sub category

*If these look familiar…they should, these are the criteria categories for C-TPAT security standards*
Risk Based Supply Chain Security

How can my company conduct a Vulnerability Assessment?

- Conduct/document *self-assessments* and evaluate the results for vulnerabilities
- Conduct/document *on-site* visits and assessments; evaluate the results for vulnerabilities (even though they are probably more credible than a self-assessment, you might have to limit the on-site assessments and limit it to those facilities with the highest risk ratings)
- Determine effectiveness by assessing: *deterrence, detection, delay* and *response* functions
- Review frequency of changes in custody and how long freight is “at rest” at any point in the supply chain
- Review any incidents or history of supply chain security matters and determine if there is an effectiveness issue
- Determine an overall Vulnerability rating (e.g. high, medium, low, etc.)
- Assign a value to that rating
Risk Based Supply Chain Security

Consequences Assessment:

An assessment of the impact of an adverse occurrence, such as loss of a business partner, to a business enterprise:

- Impact on U.S., its citizens/assets, and the company – nightmare: a WMD was found in cargo being shipped by and/or attributed to your company
- C-TPAT membership/status and lost benefits
- Value of cargo (high value, trademark, restricted, food, pharmaceuticals)
- Financial impact (more than just monetary value)
- Volume of cargo (degree of reliance on this source)
- Reputation
- Integrity
- Regulatory issues
- Quality Assurance
Risk Based Supply Chain Security

How can my company conduct a Consequences Assessment?

NOTE: You probably already have much of this information somewhere within the company, e.g. in contracting or procurement

- If this involves a business partner, ask: How critical is this business partner to your business?
- Financial value
- Quantity/Volume
- Seasonal variations, if applicable
- How could our Reputation be impacted?
- Determine an overall Consequence rating (e.g. high, medium, low, etc.)
- Assign a value to that rating
Risk Based Supply Chain Security

How can my company conduct a Risk Assessment?

• Establish a process
• Conduct a Threat Assessment
• Conduct a Vulnerability Assessment
• Conduct a Consequence Assessment
• Combine the three components to determine a Risk rating

\[ \text{Threat} \times \text{Vulnerability} \times \text{Consequences} = \text{Risk} \]
Risk Based Supply Chain Security

How can my company calculate the Risk?

T x V x C = Risk

- Assign a variant value for at least high (probably a higher number - 3), medium (2) and low (1) Threats, Vulnerabilities and Consequences.
- Multiply or add them together to combine the scores
- That will give you a Risk number which will equate to at least a high, medium or low Risk
How can I Calculate Risk?

**EXAMPLE:**

This example is determining the Risk from the perspective of an importer in the United States.

It focuses on a supply chain that starts at a factory in Mexico and ends with an importer Distribution Center in the U.S.
Risk Based Supply Chain Security

How Can I Calculate Risk? (cont.)

1. Manufacturer
   Widget Factory (WF)

2. Carrier
   Long Haul Transport (LHT)

3. Carrier
   Border Crossing Transport (BCT)

4. Distribution Facility
   Widget Distribution (WD)
Risk Based Supply Chain Security

How Can I Calculate Risk? (cont.)

Manufacturer
Widget Factory (WF)

- **Threats**: Checks with CBP, World Bank, OSAC and TAPA resulted in a score of 4 on a 1 – 5 scale (with 5 being the highest threat)

- **Vulnerability**: Self assessment and on-site assessment results in a score of 2

- **Consequence**: In-house evaluation results in a score of 4
Risk Based Supply Chain Security

How Can I Calculate Risk? (cont.)

- **Carrier**
  - **Long Haul Transport (LHT)**

- **Threats**: Checks with CBP, OSAC and TAPA resulted in a score of 4
- **Vulnerability**: Self assessment results in a score of 4
- **Consequence**: In-house evaluation results in a score of 4
Risk Based Supply Chain Security

How Can I Calculate Risk? (cont.)

 Carrier
Border Crossing Transport (BCT)

- **Threats:** Checks with CBP, OSAC and TAPA resulted in a score of 5
- **Vulnerability:** C-TPAT certified and some self assessment type information results in a score of 4
- **Consequence:** In-house evaluation results in a score of 4
Risk Based Supply Chain Security

How Can I Calculate Risk? (cont.)

Distribution Facility
Widget Distribution (WD)

- **Threats:** Checks with CBP, TAPA and McAllen Police Department resulted in a score of 3
- **Vulnerability:** Self assessment and on-site assessment results in a score of 3
- **Consequence:** In-house evaluation results in a score of 4
Risk Based Supply Chain Security

How Can I Calculate Risk? (cont.)

- Manufacturer
  - Widget Factory (WF)
  - Risk Score – 32

- Carrier
  - Long Haul Transport (LHT)
  - Risk Score - 64

- Carrier
  - Border Crossing Transport (BCT)
  - Risk Score - 80

- Distribution Facility
  - Widget Distribution (WD)
  - Risk Score - 36
Risk Based Supply Chain Security

How can my company develop a Risk-Based supply chain security management approach?

- Do not just “throw” security measures or improvements at every location -- unless you have an unlimited security budget
- Determine which facilities or supply chain partners are highest Risk and focus on lowering the Risk at these first
- It is difficult for a company or site to change a Threat, but a company/site can take steps to lower the Vulnerability and/or Consequences
- Concentrate on those Vulnerabilities and Consequences that can result in the most significant mitigation of Risk
- That is managing Risk in a Risk-Based manner!
Risk Based Supply Chain Security

Risk-Based Supply Chain Security Action Plan

- Use the Risk ratings to prioritize facilities, sites and business partners; have corrective action plans for all Vulnerability Assessments (self and on-site) or change processes to lower Consequences

- Identify:
  - Deficiencies/areas for improvement
  - Countermeasures
  - Prioritize them
  - Identify who is responsible for correcting the issue
  - Establish a deadline for implementation
  - Track corrections
  - Conduct follow-up verification
  - Recalculate Risk
Risk Based Supply Chain Security

SUMMARY:

• Your goal should be to have a Risk-Based Supply Chain Security Program
• By using sources – even open sources -- for identifying threats, the tools you should already have established for the C-TPAT program (e.g. self assessments, on-site assessments), and knowledge of your critical business processes, any company can determine their Risks
• The more qualitative and quantitative you are in assessing the Threats, Vulnerabilities and Consequences, the better your Risk Assessment will be
• When Risks are known, you can best allocate your time and resources to ensure the best possible supply chain security program for your company and make certain it meets C-TPAT requirements