**SUPPLY CHAIN SECURITY AND RISK MANAGEMENT – Draft 2 (Jan. 16, 2013)**

5 credit course, Spring quarter 2013, 11 sessions @ 3 hours

**Course Description:**

This course overviews logistics security threats and risks and the countermeasures that can be used to secure fixed assets and assets in transit. Students will become familiar with applicable domestic and international standards, laws, and regulations as well as the technologies that are used in ensuring that the supply chain is safe.

**Detailed Course Outcomes**

1. Define the threats regarding the transit and storage of goods as they are transported through the supply chain.
2. Describe the importance of the global transportation system
3. Explain the role of industry organizations, US government agencies, and applicable domestic and international standards, laws, and regulations in combating logistics threats.
4. Explain how security countermeasures are used to combat logistics security threats.

**General Session Plan and Curriculum (see following pages)**

**Session 1 - Context and Definitions**

Formal definition of supply chain security: “The application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information and personnel) from theft, damage, or terrorism and to prevent the introduction of unauthorized contraband, people or weapons of mass destruction into the supply chain” (Closs & McGarrell, 2004)

The need for security arising at the confluence of:

* + The nature of modern supply chains, incl. logistics and transportation
  + The external threat environment

1. Drivers of modern logistics and transportation:

* Domestic and international trade and consumption patterns
* Long, global and complex supply networks
* High value goods transported and stored
* Increasing global prosperity
* Cost and efficiency pressures (lean principles)
* Fragile technologies

1. Drivers of external threats:

* Human proclivity to get involved in crimes against people or property
* Human proclivity to cheat
* Human proclivity to fanaticism, extremism or radicalism
* Construction in areas prone to natural disasters
* Higher population density
* Natural disasters

Definitions of and overlap between:

* Supply Chain Management, Logistics and Transportation
* Supply chain risk management
* Supply chain security
* Security vs. Safety
* Categories of disruptions

Typical security breaches that interrupt the supply chain:

* Various intentional acts (crimes), such as:
  + Theft and robbery
  + Vandalism and intrusion
  + Terrorism and killings
  + Intellectual property rights violations (counterfeiting, piracy)
  + Kidnappings, hijackings, and maritime piracy
  + Industrial espionage
  + Intentional product contamination
* Various natural disasters, such as:
  + Geophysical (e.g. earthquakes)
  + Meteorological (e.g. storms)
  + Hydrological (e.g. floods)
  + Climatological (e.g. draughts and wildfires)
  + Biological (e.g. pests and epidemics)
* Safety relates to prevention of accidents or damage
  + Accidents can cause security threats
* How events including natural disasters or accidents often lead to security risks:
  + Compound or cascading situations
  + Opportunism

Typical consequences of security breaches (and real life, recent examples of each):

* Injuries or deaths
* Property damage
* Damage to or loss of cargoes
* Inability to meet demand and lost sales
* Lower profitability and shareholder value
* Loss of market share
* Possible bankruptcy or shut-down by the government
* Sanctions by the government, incl. fines, revocations of licenses, scrutiny
* Loss of reputation, negative PR
* Damaged careers and loss of jobs

Case example: Cold chain

**Session 2 – Analytical Frameworks**

The three supply chain flows and how they are exposed/vulnerable:

1. Goods flow (most emphasis)
2. Information flow (some emphasis)
3. Monetary flow (not much emphasis)

Definitions of “risk”:

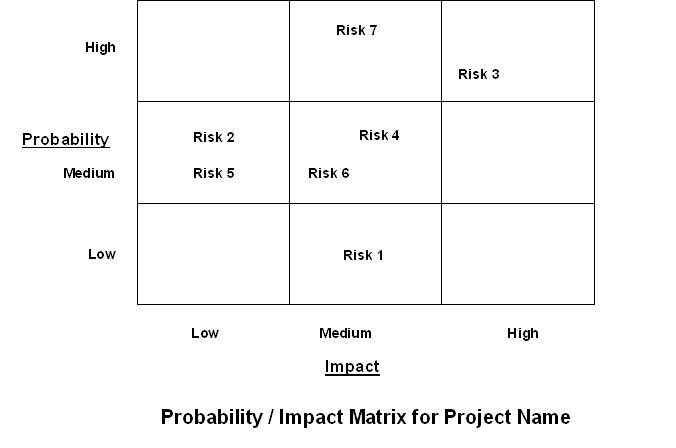
* + Subjective vs. objective
  + Risk vs. uncertainty

The “MIAMI” methodology or structure of analysis:

Part 1:

1. **Mapping** the supply chain (what is at risk?)
2. **Identifying** possible security risks (what can go wrong?)
3. **Assessing** the probability and possible impact of the security risks (how likely is it and how can it hurt us?)

Using portfolio analysis to plot possible risks in a probability vs. impact matrix:



Part 2:

1. **Mitigating** the risks through appropriate pre- and post-event procedures and actions (what can we do to avoid it or survive it?)
2. **Improving** the visibility and procedures through monitoring, learning and information (how can we be better prepared?)

Historical and recent patterns of the most severe security threats affecting logistics and transportation:

1. Domestic and global terrorism
2. Highway robberies, hijackings, piracy at sea
3. Theft
4. Vandalism
5. Intellectual property theft (copyrights, trademarks, patents)
6. I.T. threats (hacking, spyware, computer viruses)
7. Natural disasters
8. Man-made disasters (accidents) such as fires and explosions
9. Transportation and storage of hazardous materials (HazMat)

Example: The TSM (Total Security Management) framework by Ritter, Barrett and Wilson:



An example of a model that can be modified to fit the circumstances and operational parameters of the firm and supply chain.

For example, techniques such as “Six Sigma” can be used as a project management tool to help identify and analyze security threats and design appropriate solutions.

**Session 3 – The Regulatory Environment**

How efforts to stop terrorists and secure non-proliferation created new bureaucracies.

1. **Main concerns (areas of responsibility) with respect to:**
2. Export control (several agencies involved, but mostly Dept. of Commerce)

* Export Administration Regulations (EAR)
* International Traffic in Arms Regulations (ITAR)

1. Import control (several agencies involved, but mostly Dept. of Homeland Security)

* Customs
* Importer Security Filing (ISF)
* Container security initiative (CSI)
* Customs-Trade Partnership for Trade (C-TPAT)
* Product-specific restrictions:
  + FDA, USDA, ATF, DOE, DOT, EPA, etc.

1. Public safety (multi-agency responsibility; international, federal, state, county and local)

Crime prevention

Anti-terrorism

Constitutional and human rights

Patriot Act and similar counter terrorism legislation

1. **Government agencies and jurisdictions involved in logistics (cargo and transportation) security, e.g.:**

* Dept. of Homeland Security
  + Immigration and Customs Enforcement (ICE)
  + Homeland Security Investigations (HSI) and Project Shield America
  + Transportation Security Administration (TSA)
  + Federal Emergency Management Agency (FEMA)
  + U.S. Coast Guard
* Dept. of State
  + Office of Defense Trade Controls and ITAR
* Dept. of Defense
  + Defense Security Service
  + Defense Technology Security Administration
  + National Guard
  + Army Corps of Engineers
* Dept. of Commerce
  + Bureau of Industry and Security (BIS) and Export Administration Regulations
* Dept. of Treasury
  + Office of Foreign Assets Control
* Dept. of Transportation
  + Various mode-related agencies

Basic assumptions or limitations

* Security and preventative measures have to stay within prevailing law
* Cooperate with authorities and law enforcement
* Stay informed of new regulations, limitations, requirements
* Be aware of local jurisdictions and laws
* Design security measures based on a cost vs. benefits analysis

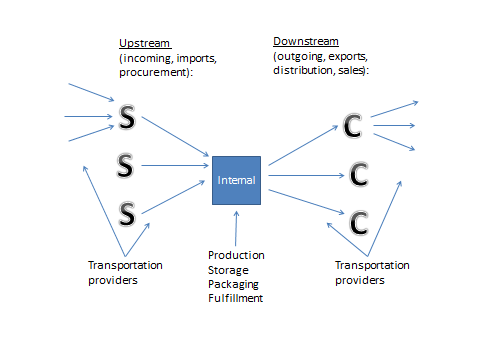
Discussion of advantages and disadvantages of a “Fortress America”

International organizations and legislative bodies involved in transportation and trade security:

* United Nations
* World Trade Organization
* World Health Organization
* International Air Transport Association
* International Atomic Energy Agency
* International Maritime Organization, SOLAS
* NAFTA
* European Union
* ISO (International Standards Organization)
  + ISO 28000

**Session 4 – Mitigation of Security Risks**

Security measures throughout the supply chain and dealing with the flow of goods:



Upstream:

1. Dealing with suppliers and second-tier suppliers
2. Choosing modes and dealing with logistics and transportation providers
3. Dealing with customs regulations for imports

Internal:

1. Dealing with receiving cargoes
2. Dealing with storing merchandise
3. Dealing with securing facilities
4. Dealing with order fulfillment (pick and pack)
5. Dealing with shipping cargoes

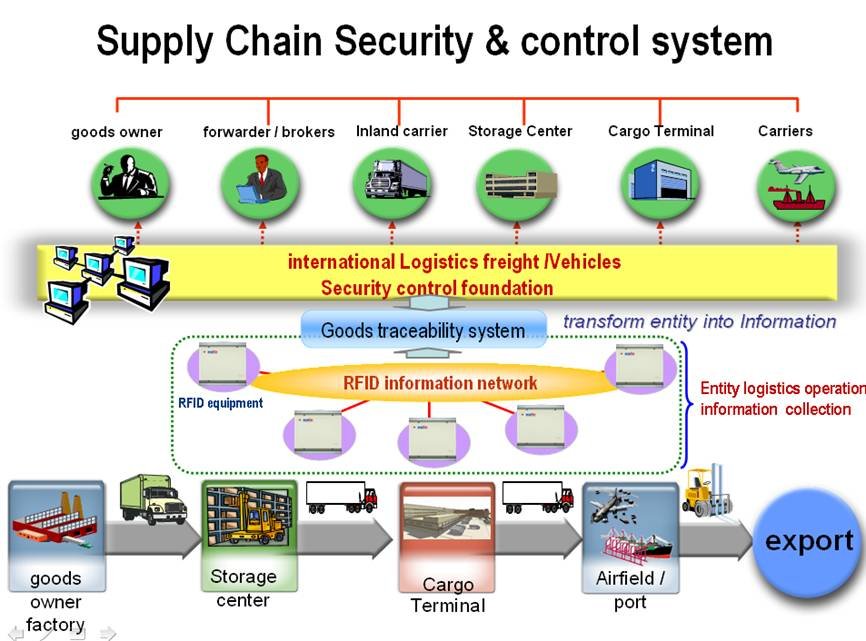
Downstream:

1. Choosing modes and dealing with logistics and transportation providers
2. Dealing with documentation issues
3. Dealing with export compliance for exports
4. Dealing with customers
5. Dealing with reverse logistics (returns, warranties, repairs)

Security measures chart

* Transportation security
* Facilities security
* Cargo security
* Information security

Example illustration:



Source: <http://www.itri.org.tw/eng/UpFile/_userfiles/image/Supply%20Chain%20Security%20Control%20System.jpg>

**Session 5 – The Upstream Focus (dealing with suppliers and incoming cargoes); Air and Ocean**

Upstream focus:

1. Securing the supplier network

* Know your suppliers
* Contractual obligations
* Train, certify, inspect suppliers
* Preapproved suppliers under C-TPAT
* Prescribe proper packaging, stowing and shipping methods
* Case studies?

1. Securing the inbound transportation network

Modes:

* **Air cargoes and its security measures:**
  + Documentation
  + What is shippable
  + Deadlines
  + Scanning
  + Protecting airports
  + Applicable domestic and international legislation
  + Mitigation best practices
* **Ocean freight and its security measures:**
  + Documentation
  + Deadlines
  + Scanning and inspections
  + CSI and ISF
  + Seals
  + Protecting seaports
  + Applicable domestic and international legislation
  + Mitigation best practices

**Session 6 – Upstream focus; Road, Rail and Intermodal**

Modes (continued):

* **Road transportation (trucking) and its security measures:**
  + Documentation
  + Driver screening and qualifications
  + Safety regulations (equipment and hours of service rules)
  + Positioning systems (GPS)
  + Crossing the Canadian and Mexican borders
  + Protecting truck terminals
  + Applicable domestic and international legislation
* **Rail transportation and its security measures:**
  + Documentation
  + Operator screening and qualifications
  + Safety regulations (equipment, tracking and signage)
  + Protecting rail terminals
  + Applicable domestic and international legislation
* **Intermodal considerations and challenges**
  + Transfers of cargoes and containers between operators and modes
  + Dealing with 3PL’s

Possible guest presenter.

**Session 7 – Internal focus: Warehouses, Distribution Centers**

Internal focus:

Protecting warehouses, distribution centers, production facilities and terminals

* Electronic tracking systems (bar codes, RFID)
* Access control for vehicles and personnel
* Warehouse layouts, zones, separators
* Specialized handling and storage of hazardous, valuable or sensitive items
* Barriers and deterrents to prevent theft and vandalism
* Proper packing and labeling procedures for outgoing cargoes
* Documentation procedures

Possible Interactive Student Project: Research security issues for each transportation mode and facilities management, and contribute regulations and best practice suggestions:

|  |  |  |
| --- | --- | --- |
| **PHASE:** | **Laws & Regulations:** | **Best practices:** |
| **Upstream (inbound):** |  |  |
| **AIR** |  |  |
| **OCEAN** |  |  |
| **ROAD** |  |  |
| **RAIL** |  |  |
| **INTERMODAL** |  |  |
| **Internal (facilities management):** |  |  |
| **RECEIVING** |  |  |
| **STORAGE, INVENTORY MGMT** |  |  |
| **FULFILLMENT** |  |  |
| **SHIPPING** |  |  |
| **Downstream (outbound):** |  |  |
| **AIR** |  |  |
| **OCEAN** |  |  |
| **ROAD** |  |  |
| **RAIL** |  |  |
| **INTERMODAL** |  |  |

**Session 8 – Downstream focus: Shipping and Distributing the goods**

Downstream focus

* Securing the customer network
  + Know your customers
  + Documentation issues, especially export control
* Transportation issues
  + Selecting the proper transportation modes
  + Dealing with freight forwarders and 3PL’s
* Retail operations
  + Store security for retail operations (theft control)
  + Link to pertinent sources or articles regarding store management
* Reverse logistics
  + Handling returns, warranties, damaged goods

Possible field trip.

**Session 9 – Securing the Information and Monetary Flows**

Security measures related to the Information flow:

* Protecting electronic data and transmissions
  + Network and computer security
  + In-house servers and data storage vs. cloud computing and storage
  + Backup and redundancy procedures
  + Data privacy
* Protecting intellectual property rights
  + Safeguarding secrets, recipes, patents, designs
  + Copyright and trademark protection

Security measures related to the Monetary flow:

* Safe payments procedures
* Secure transportation of cash and cash equivalents
* Anti-corruption and anti-bribery procedures

Insurance and limitations:

* Cargo insurance and exceptions
* Property insurance
* Liability insurance
* Credit risk insurance
* Business interruption insurance
* Federal insurance provisions

**Session 10- Emerging Technologies**

A closer look at security technologies

* RFID (radio frequency identification):
  + Tracking and tracing
  + Matching
  + Access control
* Global Positioning Systems (GPS) and satellite technologies
  + Tracking and tracing
  + Locating
* Biometric scanners (finger prints, retina, breathalyzers)
  + Access control
* X-ray scanners
  + Anti-terrorism
  + Anti-contraband
  + Anti-smuggling
  + Verification
* Radioactive material detectors
  + Anti-terrorism
  + Anti-smuggling
  + Public safety
* Robots
* Artificial intelligence

Guest presenter on a current technology.

**Session 11- Looking ahead and streamlining the supply chain**

Discussion of the most realistic security threats for the next decade:

* International terrorism
* Domestic terrorism
* Wars, civil unrest, riots
* Climate change and global warming
* International criminal gangs (theft, hijackings, counterfeiting, cyber crime)
* Others?

Discussion of good supply chain management risk practices and how both performance and security are improved by implementing preventative strategies and business continuity planning, leading to more resilient and agile companies and supply chains:

* Supply chain visibility
* Supply chain flexibility
* Supply chain buffers and redundancies (backups)
* Supply chain collaboration (upstream and downstream)
* Supply chain simplification and standardization
* Supply chain postponement (modularization)

Possibly a case study and discussion.

Possibly presentation of student projects.