Supply Chain Risk Management
Industry Approaches

15 October 2012
Industry approaches to SCRM

• Supply chain risks
• About the Supply Chain Risk Leadership Council
• SCRM best practices
• Where we are headed
The SCRM Challenge

- How to secure supply chains in an environment where manufacturers barely touch the products they make?
- How to get consistent SCRM processes across multiple commodities and customers?

Boeing 787 Supply Chain

Subcontracted assemblies included wing manufacture (Mitsubishi Heavy Industries, Japan, central wing box) horizontal stabilizers (Alenia Aeronautica, Italy; Korea Aerospace Industries, South Korea); fuselage sections (Global Aeronautica, Italy; Boeing, North Charleston, USA; Kawasaki Heavy Industries, Japan; Spirit AeroSystems, Wichita, USA; Korean Air, South Korea); passenger doors (Latécoère, France); cargo doors, access doors, and crew escape door (Saab, Sweden); floor beams (TAL Manufacturing Solutions Limited, India); wiring (Labinal, France); wing-tips, flap support fairings, wheel well bulkhead, and longerons (Korean Air, South Korea); landing gear (Messier-Dowty, France); and power distribution and management systems, air conditioning packs (Hamilton Sundstrand, Connecticut, USA). Boeing is considering bringing construction of the 797-9 tail "in house"; the tail of the 787-8 is currently made by Alenia.

(Source: Wikipedia.org)

Apple iPhone Supply Chain

Sources:
- Abilla, Pete, “The Apple iPhone Supply Chain”, January 18, 2007; accessed online, 25 August, 2010
- “iPhone: Who’s the Real Manufacturer? (It isn’t Apple)”, TEXYT, June 26, 2007; accessed online August 25, 2010

F-35 Supply Chain

Sources:
- Abilla, Pete, “The Apple iPhone Supply Chain”, January 18, 2007; accessed online, 25 August, 2010
- “iPhone: Who’s the Real Manufacturer? (It isn’t Apple)”, TEXYT, June 26, 2007; accessed online August 25, 2010
Supply Chain Risks can take multiple forms.

- Financial risks—supplier failure, customer default, bad debt, etc.
- Demand, supply, or market variability—unforeseen spike or drop in demand, market shifts, new technologies, etc.
- Quality risks—poor quality items, non-spec materials, embedded code errors, etc.
- Natural disruptions—severe weather, natural disasters, etc.
- Accidental disruptions—transportation accidents, production accidents, etc.
- Man-made disruptions—labor disputes, protests, etc.
- Malicious disruptions—tactical strikes, vandalism, hacking, etc.
- Cyber security—malicious code, counterfeits, etc.
SCRLC Member Companies
(not all inclusive)
**SCRLC Structure**

**SCRLC Governance Body**
- SCRLC Direction and Operation, and Managing Partnerships with other Organizations

**SCRLC Products**
- Strategy and Plan
- SCRM Guidance
- Best Practices
- Tools (eg. spreadsheets)
- Maturity Model
- White Papers
- Training Materials
- FAQ’s
- Consistency and harmonization

**Work Product Development**
- BP Sub-teams
- Assessment
  - Identification
  - Analysis
  - Evaluation
- BCM/BCP
- EA/ER
- Crisis Mgmt
- Security
- Compliance
- Metrics
- Resiliency framework
- Implementation
  - Organization
  - Training
  - Information needs
  - Integration w/ business processes
  - Metrics
- Maturity Model
- Training

* Special purpose teams as needed to create products

**Communication and Influencing**
- Outreach
- Influencing
- Conferences and meetings
- Web site and content
- Technology platform

* Special purpose teams as needed to design and implement

**SCRM Foundation Principles**
- Common language, processes, concepts, and frameworks
SCRM Best Practices

• Developed by practitioners from industry leading companies

• Contents
  – Executive Summary
  – SCRM Overview
  – Internal and external environments
  – Risk assessment
  – Risk treatment
  – Monitoring
The foundation: ISO 31000

ISO 31000:2009
Risk Management – Principles and Guidelines

Establish the Context

Risk Assessment
- Risk Identification
- Risk Analysis
- Risk Evaluation

Risk Treatment

Monitoring and Review

ISO Guide 73
Risk Management Vocabulary

Also draw from ISO 28000 series on supply chain security
Internal and external environments

• Understand your supply chain environment
  – Who is involved
  – What do they do
  – Where do they do it

• In other words…map it!

Don’t neglect communication and information flow!

LMĪ
Risk assessment

• Identify your risks
  – What can disrupt your supply chain?
  – Resources: SCRLC, ISO 31010, BS 31000

• Analyze and evaluate your risks
  – Determine likelihood and consequence
  – Alternative approach—lost node or route
Risk treatment

- Treatment is not always mitigation
- Balance prevention and response
- Don’t just focus on avoiding the bad—how can you benefit from the event?
- Don’t forget to include recover!
Monitoring

- Test, drill, and update
- Monitor risk precursors
- Communicate, communicate, communicate
- Even if your supply chain doesn’t change, the rest of the world does
What’s next?

• Tools for risk management
  – Visibility
  – Simulation and measurement
  – Monitoring and alerts

• Emerging risks
  – Cyber/IT (embedded and corporate)
  – Regulatory (e.g., conflict minerals, REACH, etc.)
  – Climate change/sustainability
  – Social media

• Approaches for the hard problems
  – Visibility
  – Multi-tier collaboration/coordination
  – Increase development and use of standards
Thank you!

Taylor Wilkerson
twilkerson@lmi.org
703-917-7438