Agenda

• Overview: Defense supply chain security & risk management
• Special concerns & issues in the defense supply chain
• Supply chain security management (SCSM): Equations, frameworks, models, processes
• Best practices from the private sector:
  – Cisco
  – McAfee
  – Pharmaceuticals Industry
• Questions - discussion
Defense supply chain security: CPPPE research paper

Key Findings – Highlights

• DoD’s supply chain: Highly complex, geographically dispersed, operationally volatile, high risk

• Threats range from benign to catastrophic

• Definition of SC 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."

• Any definition must incorporate three unique, but interrelated constructs: risk, protection and safety.
Resiliency white paper series
Most common security problems

Source of vulnerabilities

- 60% of all supply chain security problems involve poor transportation-related security
- 20% involve poor security at the manufacturing site, including poor access controls and poor security practices within the shipping and receiving departments
- 10% involve poor security at distribution nodes
- 10% - other

90% of the time, the security weaknesses were well known internally by staff.

Illustrative Supply Chain Risk & Impact

Source: Transport Intelligence
DoD’s supply chain risk is escalating

• Evolution to a highly geographically dispersed network model has amplified security risk significantly.
• This was true in 2012; even more true in 2016
• WHY?
  – Supply chain operating practices (e.g., lean, just in time, inventory optimization, outsourcing, contract manufacturing) reduce costs but decrease flexibility/resiliency; increase vulnerability
  – DoD’s reliance on a global supply base puts it at risk from counterfeit parts, supply discontinuity and disruption, quality failures, and so on
  – Huge global scope & complexity – Thousands of suppliers/service providers
  – Greater dependence on IT & technology systems & products increases vulnerabilities from cyber disruption and attack, malware, security breaches/hacking, compromised components, and compromised networks.

Source: Transport Intelligence
Visibility black holes = risk

Traditional linear supply chain:
• No visibility to the lowest or "nth" supplier
• Information black holes inject time and risk into the supply chain
• Results - excess inventory, obsolescence, security risk, production shutdowns, business interruption, increased costs and revenue decline.
Traditional supply chain

Traditional approach with information latency and demand distortion
Example: Network model with real-time visibility

End-to-end lead time and flow*

<table>
<thead>
<tr>
<th>Approach</th>
<th>Material</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional</td>
<td>43 days</td>
<td>29 days</td>
</tr>
<tr>
<td>Demand-driven</td>
<td>43 days</td>
<td>1 day</td>
</tr>
</tbody>
</table>

Source: One Network and Tompkins International.
Supply Chain Security

RISK FRAMEWORKS & MODELS
Supply chain security risk equation

Fundamental premise:
Supply chain security can be viewed, measured and managed in the context of a risk management equation.
Quantification frameworks:  
End-to-end supply chain security risk assessment

<table>
<thead>
<tr>
<th>Tier</th>
<th>Threats</th>
<th>Vulnerabilities</th>
<th>Consequences</th>
<th>Severity Rating – Apply to each identified element</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic Tier</td>
<td>Terrorism, nation-state “attack”, cyber warfare, massive supply disruption</td>
<td>Critical infrastructure, core supply lines</td>
<td>Shut down of single or multiple critical infrastructure sectors/components/geographies/capabilities</td>
<td>High, Moderate, Low, None</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational Tier</td>
<td>Terrorism, nation-state “attack”, cyber warfare, natural disasters, intrusion/counterfeiting/diversion</td>
<td>Supply chain operating capability, continuity, performance, flows</td>
<td>Widespread supply chain security breach with major supply chain disruption. Inability to accomplish mission.</td>
<td>High, Moderate, Low, None</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tactical Tier</td>
<td>Terrorism, criminal or activist activity, natural disasters, supply disruption, cargo/facility/personnel security, supply operations, on-ground readiness</td>
<td></td>
<td>Cost of goods lost, support interruption, damage/injury, loss of life</td>
<td>High, Moderate, Low, None</td>
</tr>
</tbody>
</table>
Framework incorporates 5 primary principles utilized to achieve desired outcomes.

1. **Detect**: Identify actors, identify threat/vulnerability – continual surveillance

2. **Prevent**: Eliminate threat/vulnerability through preventive measures, alternative solutions, etc.

3. **Delay**: Postpone occurrence through intervention (e.g., “patches”, labor workarounds, contingent capacity)

4. **Respond/recover**: Manage occurrence and recovery from it

5. **Measure/improve performance**: Measure outcome of intervention, identify improvements, implement

© 2016 lharrington group llc
**SCOR SCRM model**

The SCOR SCRM Model provides a five-step process framework for identifying and mitigating supply chain risk.

Key takeaways - best practice:
- Empirical quantification of value at risk and time to recover.
- Risk mitigation response tiered appropriately to value at risk and time, cost and benefits of mitigation.

1. Define the supply chain
   - Use SCOR to map the supply chain
   - Identify processes, places, and participants

2. Analyze the supply chain
   - Determine the measures for risk
   - Set risk priorities according to risk strategy

3. Assess the supply chain risks
   - Identify risks at and between each location
   - Value at Risk to quantify the risk

4. Mitigate the supply chain risks
   - Prioritize risk for mitigation
   - Calculate time, cost, and benefit of mitigation

5. Implement the mitigation measures
   - Plan implementation projects
   - Secure resources for implementation

SCSM operationalized

This schematic illustrates the operational attributes that could make up a SCSM program. The “execution” activities – in the rectangles – support the core attributes (e.g., production/ sourcing, cargo, etc.) of a supply chain.

- Supply risk management
- Contingent source contracts
- Supply protection
- Supplier quality/security program (e.g., counterfeits)
- Supply performance contracting
- Supplier security processes
- IP protection, product tampering protection

- Facility protection
- Access control
- Facility monitoring
- Warehouse layout
- Inventory management and control

- Prevention detection, anomaly reporting
- Inventory control
- Cargo inspection
- Cargo tracking
- Anti-tampering devices

- Background checks
- Training
- Roles & responsibilities
- Information dissemination
- Security culture

- Information quality & data management
- IP, business information protection (e.g., cyber attacks, authentication)
- Recordkeeping
- Data exchange with external parties
- Use of international standards for data mgt.

- Risk surveillance
- Business continuity plans
- Formal security strategies
- Emergency control centers
- Incident management & mitigation
- Continuous improvement

Adapted from Business Alliance for Secure Commerce
Examples

– Cisco
– McAfee
– Pharmaceutical industry
Cisco

• Securing the supply chain at Cisco is about managing TWO key things:
  – Value at risk (VAR)
  – Time to recover (TTR)
• Cisco’s control tower approach
Understanding supply chain disruptions

- Component Supply Disruption
- Quality Issue
- Bankruptcy
- Gulf Coast Hurricane
- Labor Disruption
- Taiwan Earthquake
- Japan Earthquake
- West Coast Earthquake
- Flood
- Pandemic

Likelihood:
- Moderate
- Severe
- Extreme

© 2016 lharrington group llc
Global event impact severity map
Chengdu crisis management response

Customer Impact
- Product A
- Product B
- Product C
- Product D

Partner Impact
- No Impact (CM 1, CM2, CM3, CM4)
- No Impact (SLC)
- Moderate Impact (4 suppliers)

Max Rev Impact
TTR: XX Weeks
Max/ Revenue Impact: $XXM
Cisco’s resiliency pillars

**Time to Recover (TTR):** number of weeks required to restore 100% operational output following a supply chain disruptions

- **Mfg TTR:** Alternate site readiness
- **Test TTR:** Lead-time programs and/or inventory for test equipment
- **Component TTR:** 2nd source, alternate supplier site and/or inventory

© 2016 lharrington group llc
McAfee: Protection through obfuscation

- Create a global supply chain configured for late-stage postponement
- How?
  1. Secure components from multiple locations via partners
  2. Assemble, convert into near-finished product at strategic locations in Europe, North America, Asia
  3. Secure order comes in
  4. Final assembly and configuration done at the very last minute – can be as little as 20 minutes
  5. Immediate shipment to customer via trusted distribution partner.

- Result: Impossible to know beforehand what a product is or where and to whom it’s headed. Obfuscation deters adulteration/intrusion.
**U.S. Drug Supply Chain Security Act**

- Signed into law November 27, 2013
- Establishes national system for tracing pharmaceutical products
- Immediately preempts all state laws, regulations and requirements for tracing products through the supply chain
- Applies to prescription drugs in finished dosage for human use
- Sets national licensing standards for wholesale distributors and third-party logistics providers
- Builds to an electronic, package-level traceability system over a 10-year period

**System in Action**

- Full traceability system, without end-point authentication
- Does not require pharmacies to verify serial numbers before patient dispense
- Focus on enabling tracking of transactions
- Verification will not be routine, except during returns and investigation of suspect product
- Unlike non-U.S. models, single government repository not likely

**November 2017**
- Drugs must be serialized by manufacturers
- Certain investigation and returns verification requirements will include verifying serial numbers

**January 1, 2015**
- Lot-level traceability system

**November 27, 2023**
- Transition to electronic, interoperable traceability system at package level
Conclusion

AN EVOLUTIONARY PROCESS
Supply chain resiliency maturity model

Four Stages

Stage 1 – React
- Individual functional approach to supply chain management and ad-hoc, reactive management of risk
- Little integration across functional boundaries
- High duplication of activities
- Internally and externally disconnected processes
- Lack of coordination with supply chain partners
- Limited supply chain visibility

Stage 2 – Anticipate
- Cross-functionally organized
- Internal processes are integrated
- Structured visibility between functions
- Alignment of performance objectives
- Risk management processes are documented and integrated internally
- Basic threats and vulnerabilities are analyzed
- Risk management activities, such as scenario planning and product postponement, help the organization begin to anticipate volatility more effectively. The focus, however, remains largely internal.

PwC and the MIT Forum for Supply Chain Innovation, 2013
Supply chain resiliency maturity model

Stage 3 – Collaborate

- External collaboration and proactive risk sharing and response
- Information sharing is extensive and visibility is high, geared to set up sensors and predictors of change and variability
- Better visibility enables the organization to proactively design and execute response mechanisms in collaboration with key external partners
- Risks are formally quantified
- Suppliers and partners are monitored for resilience levels and business continuity plans are created.

Stage 4 – Orchestrate

- Companies are fully aligned with their supply chain partners on key value dimensions across the extended enterprise
- Individual strategies and operations are guided by common objectives
- Supply chain is fully flexible to interact and adapt to complex dynamic environments
- Supply chain risk strategy is segmented to value at risk (e.g., financial loss, market share loss, damage to brand)
- Tiered response playbooks are developed to reflect this segmentation.
Research Links and Contact Info

- Defense Supply Chain Security: Current State and Opportunities for Improvement

- Performance Based Logistics: The Case of the Navy Aviation Tires Program

- HIMARS: A High-performance PBL


- [http://www.cpppe.umd.edu/](http://www.cpppe.umd.edu/)
Thank you!

Questions?

CONTACT INFORMATION: lisa@lharringtongroup.com ♦ lharring@umd.edu ♦ PHONE: 410.725.6198