

DEFENSE SUPPLY CHAIN SECURITY & RISK MANAGEMENT: PRINCIPLES & PRACTICE

Lisa Harrington
President, Iharrington group llc
Associate Director – Supply Chain Management Center
Robert H. Smith School of Business
University of Maryland

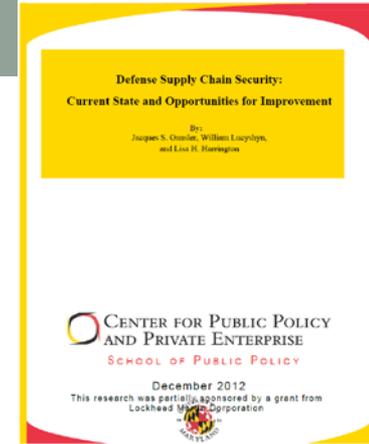
June 26, 2014
NDIA Supply Chain Summit



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
- Case studies:
 - Cisco
 - McAfee
 - Pharma
- 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:

"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.

Most common security problems

Source of vulnerabilities

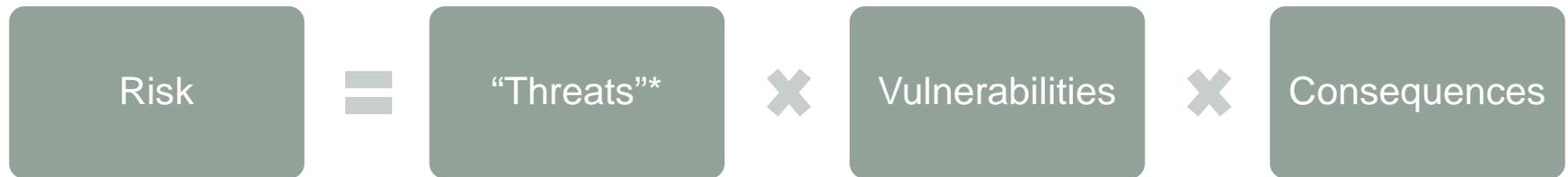
- 60 percent of all supply chain security problems involve poor transportation-related security
- 20 percent involve poor security at the manufacturing site, including poor access controls and poor security practices within the shipping and receiving departments
- 90 percent of the time, the security weaknesses were well known internally by staff.

Risk escalation in DoD's supply chain

Evolution to a highly geographically dispersed network model has amplified security risk significantly. Reasons include:

- Supply chain operating practices (e.g., lean, just in time, inventory optimization, outsourcing) reduce costs but decrease flexibility/resiliency
- 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 – 1000s of suppliers/service providers
- Dependence on IT increases vulnerabilities from cyber disruption and attack, malware, security breaches/hacking, compromised components, and compromised networks.

Supply chain security risk equation



Supply chain security can be viewed, measured and managed in the context of a risk management equation.

*Threats can also include natural disasters, power losses, etc.

End-to-end supply chain security risk assessment & quantification

- Identify DoD physical supply chain security issues
- Assign level-of-impact value to each issue (high, moderate, etc.)
- Use values to prioritize supply chain security investments and interventions.

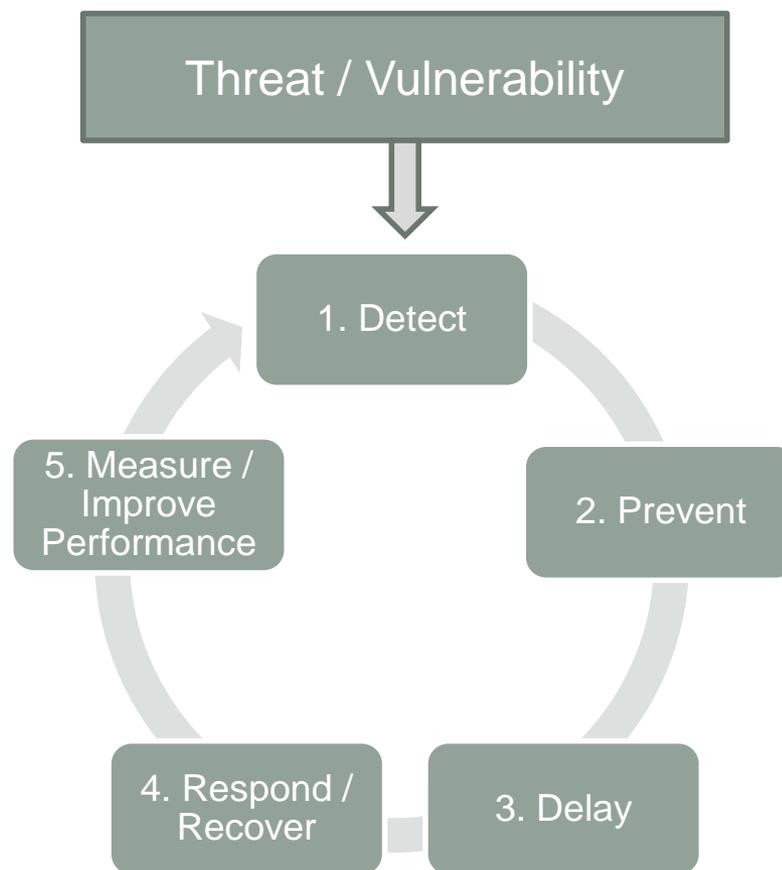
	Physical Supply Chain	Severity Rating – Apply to each identified element
Strategic Tier	<p>Threats: Terrorism, nation-state “attack”, cyber warfare</p> <p>Vulnerabilities: Critical infrastructure</p> <p>Consequences: Shut down of single or multiple critical infrastructure sectors</p>	<p>High</p> <p>Moderate</p> <p>Low</p> <p>None</p>
Operational Tier	<p>Threats: Terrorism, nation-state “attack”, cyber warfare, natural disasters</p> <p>Vulnerabilities: Supply chain operating capability, continuity, performance</p> <p>Consequences: Widespread supply chain security breach with major supply chain disruption. Inability to accomplish theater mission.</p>	<p>High</p> <p>Moderate</p> <p>Low</p> <p>None</p>
Tactical Tier	<p>Threats: Terrorist, criminal or activist activity, natural disasters</p> <p>Vulnerabilities: Cargo/facility/personnel security</p> <p>Consequences: Cost of goods lost, support interruption, damage/injury</p>	<p>High</p> <p>Moderate</p> <p>Low</p> <p>None</p>

Supply chain security process improvement framework

- Supply Chain Security Management (SCSM) focuses on how to make security measures more effective and, hence, reduce the three risk equation variables.

- The SCSM Process Improvement 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



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

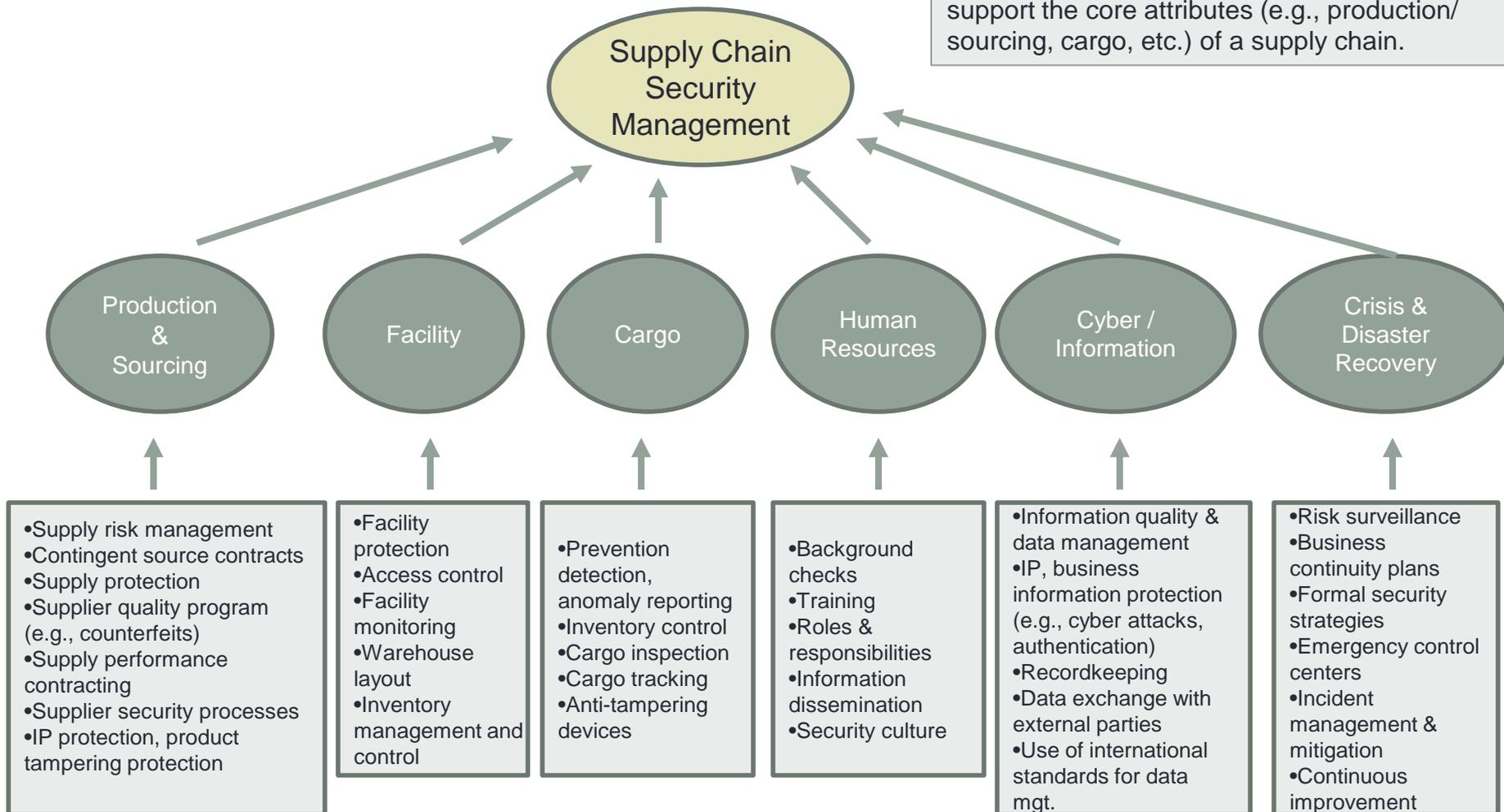
- Prioritize risk for mitigation
- Calculate time, cost, and benefit of mitigation

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.



Sample supply chain security program elements

Category	Physical Supply Chain – Program Elements
Physical security	<ul style="list-style-type: none"> • Physical deterrents • Process/procedures • Documentation • Continual monitoring, sensors
Access control	<ul style="list-style-type: none"> • Secure identification • access hierarchies and controls • Intrusion prevention
Personnel security	<ul style="list-style-type: none"> • Screening • Background checks • Procedural
Education & training	<ul style="list-style-type: none"> • Ongoing security training – all levels
Procedural security	<ul style="list-style-type: none"> • Documentation & manuals • Standardized function-specific procedures
IT security	<ul style="list-style-type: none"> • Secure access control • Accountability
Business partner security	<ul style="list-style-type: none"> • Documented security guidelines • Contractual requirements
Transportation security	<ul style="list-style-type: none"> • Inspection procedures • Cargo securement • Chain of custody protection • Documentation

This chart highlights key components of a model supply chain security program as applied to the *physical supply chain*.

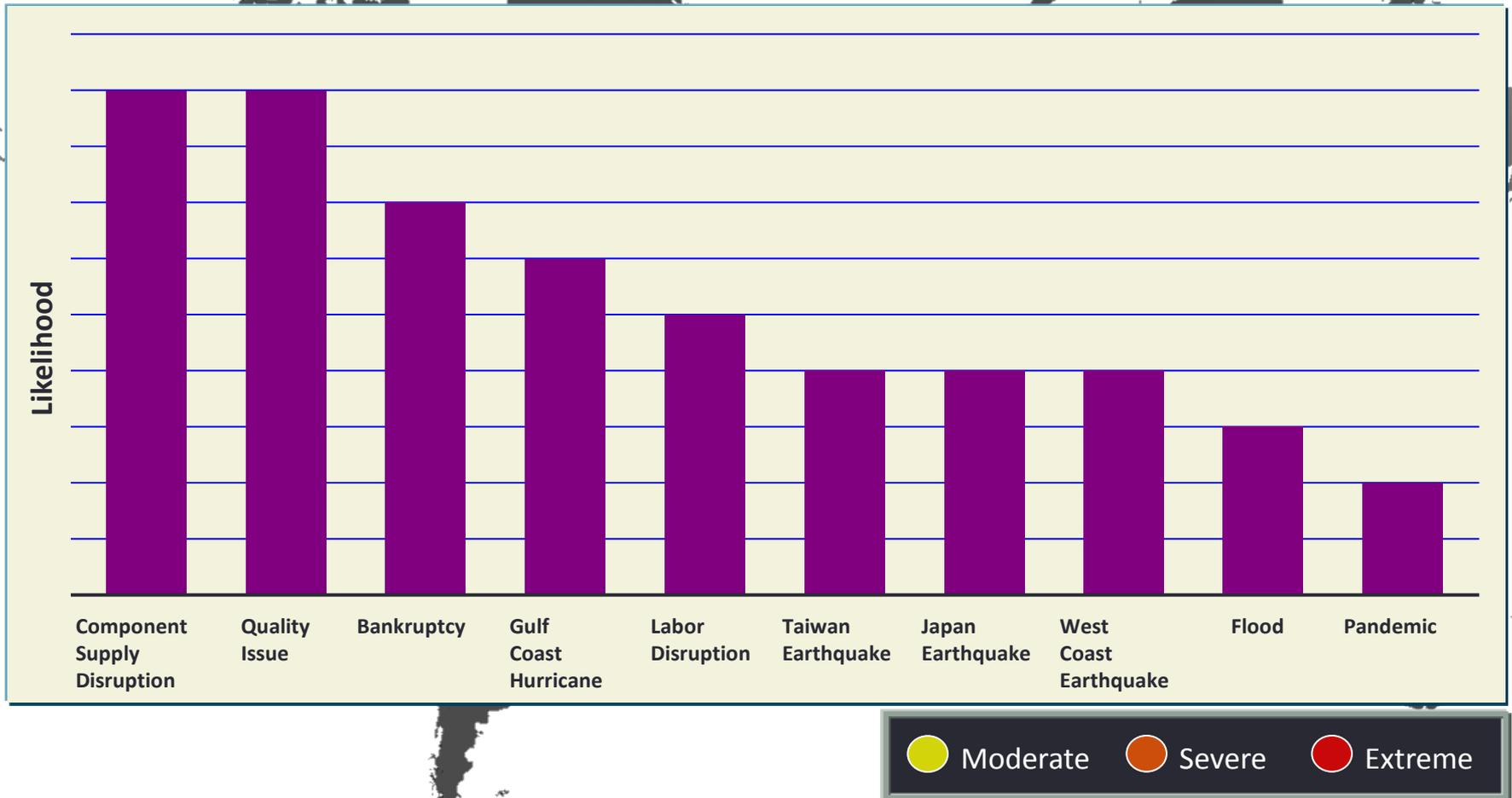
Case Studies

- Cisco: Supply chain security/risk governance structure and supporting architecture
- McAfee: Supply chain security
- Pharma industry: Counterfeits

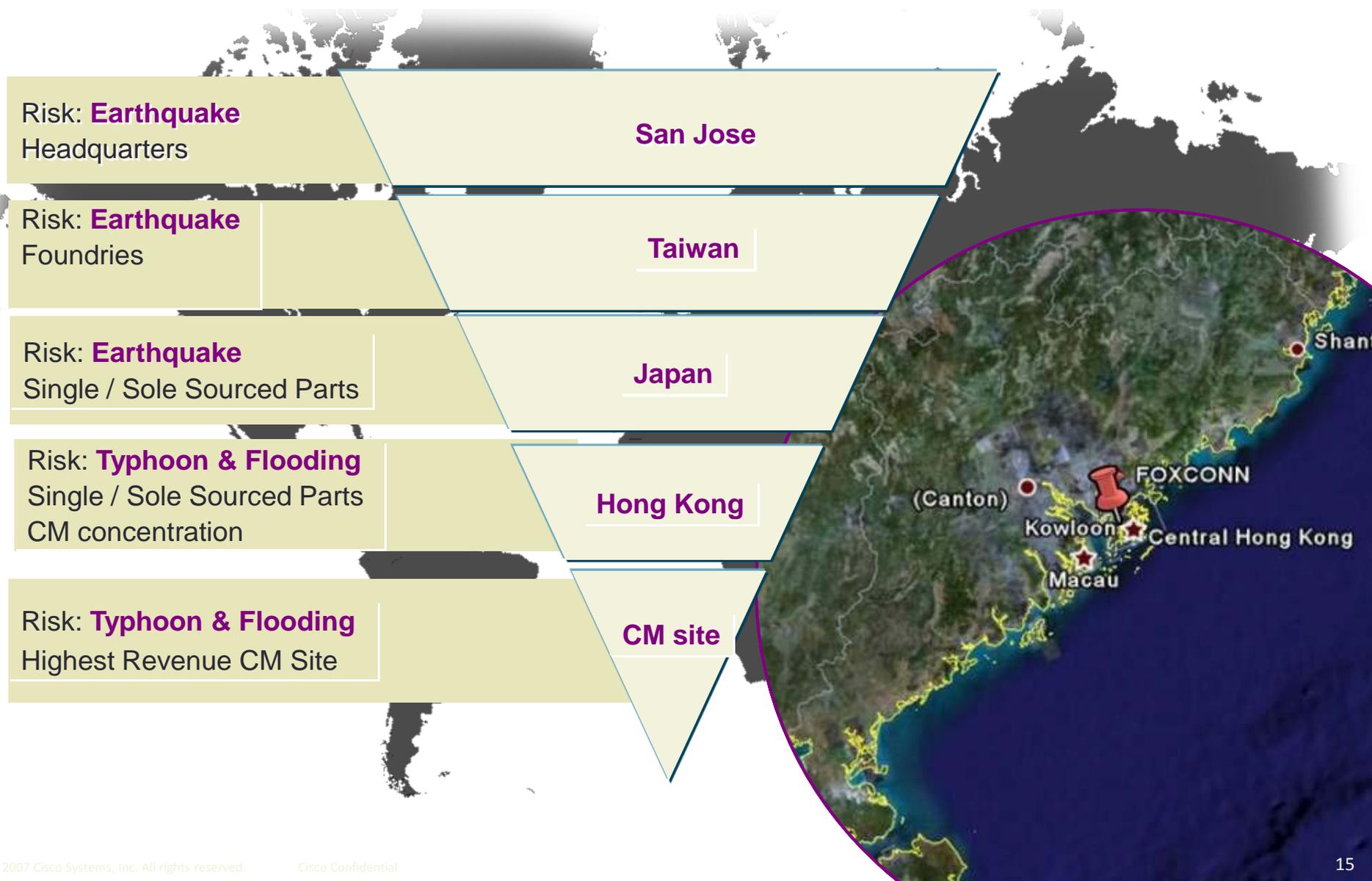
Cisco

- Securing the supply chain at Cisco is about managing TWO key things:
 - Value at risk
 - Time to recover
- Cisco's control tower approach

Understanding supply chain disruptions



Event severity exposure by location



Chengdu crisis management response

Customer Impact

- Product A
- Product B
- Product C
- Product D

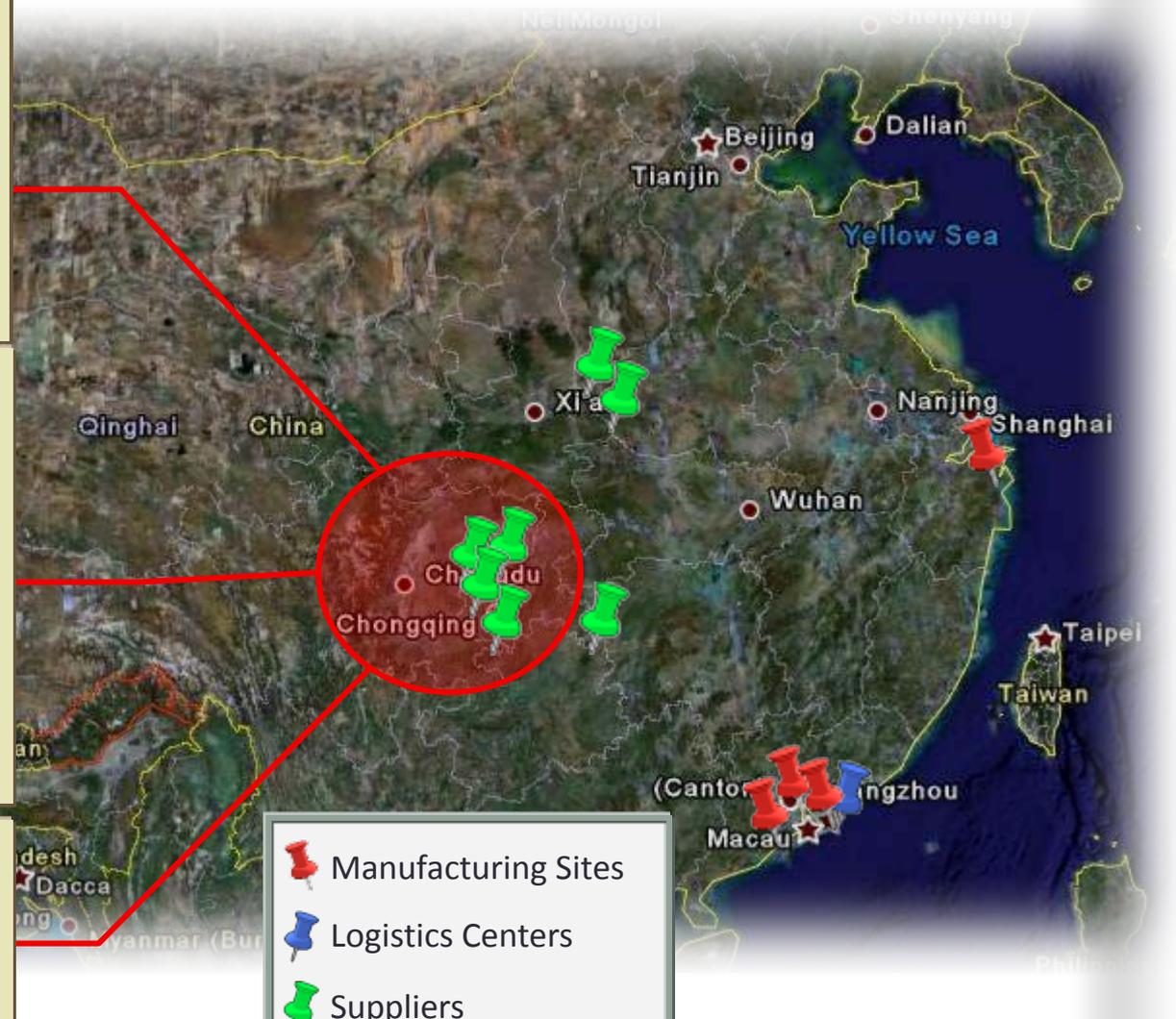
Partner Impact

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

Max Rev Impact

TTR: XX Weeks

Max/ Revenue Impact:
\$XXM



-  Manufacturing Sites
-  Logistics Centers
-  Suppliers

McAfee's supply chain security approach

- The cyber security threat:
 - Jeopardizes IT products – hardware and software
 - Intrusion
 - Injection of viruses/surveillance/other while product is moving through the supply chain – Stuxnet, Aurora, Night Dragon, etc.
 - Jeopardizes the supply chain itself
 - Puts McAfee and its customers at high risk

“More than natural disasters, financial instability, or political upheavals, what keeps me up at night is the fear that bad guys are injecting into products bad stuff that can disrupt, bring down, or steal confidential information from networks.”

What would you do?

- What steps would you take to protect McAfee's products throughout the supply chain?
- Jot down 2 ideas

McAfee: Protection through obfuscation

- What do you think this means?
- McAfee's solution: 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.

McAfee: Other practices

- Inventory keeps moving. Inventory at rest is inventory at risk
- Keep inventory levels and backlogs as low as possible
- Trusted regionalized partners – rigorous partner requirements, audits, verifications
- A “cell” strategy in the regionalized supply chain
- What ideas or practices work for you?

Pharma industry's approach

- Issue: Counterfeiting, adulteration, diversion
- Solutions:
 - Signal detection and response
 - Supplier quality management – rigorous, documented, audited
 - Logistics/transportation partner selection
 - ISO 28002:2011 – security management systems for the supply chain
 - Systematic process to enhance prevention, protection, preparedness, mitigation, response, continuity of operations and recovery from disruptive incidents

Pharma – other approaches

- Physical security of facility
- Procedures for handling and destruction of waste, particularly rejected product and packaging components.
- Procedures for the secure handling and storage of the product security features such as tamper evident labels, holograms, and other components including packaging materials
- Procedure for the secure storage and control of product security specifications and manufacturing formulas
- Adherence to company and/or site specific procedures for the handling of suspected counterfeit events
- Review of production yields, capacity, and/or product amounts compared with raw material purchases
- Training and qualification of personnel directly involved in product security and counterfeit detection.
- Well-defined logistics and transportation security systems and controls.

QUESTIONS – DISCUSSION?

Thank you!