Supply Chain Security & Risk Management: New Thinking

Lisa Harrington
President, lharrington group LLC
and
Faculty Research Associate
Center for Public Policy and Private Enterprise
University of Maryland
June 7, 2017
Agenda

• Overview: Supply chain security & risk management – an escalating concern

• Countermeasures:
  • Legislative
  • Voluntary frameworks
  • Industry efforts

• New thinking: What’s being done?
  • The plug-and-play supply chain
  • Cisco – next generation

• Questions
How Do You Define 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, malware or weapons of mass destruction into the supply chain."

• The supply chain consists of BOTH the physical and cyber supply chains

• Supply chain risk management & security are inextricably linked
Supply Chain Risk is Escalating

- Growing concerns about disruption
- 2014 BCI Horizon scan report of top concerns
  - Supply chain disruption - #16

- 2015 BCI Horizon scan report of top concerns
  - Supply chain disruption - #5
Why More Risk? One Word: Complexity

MIT Study

Agree/strongly agree

CHANGES IN THE EXTENDED SUPPLY CHAIN NETWORK CONFIGURATION OCCUR MORE FREQUENTLY

DEPENDENCIES BETWEEN SUPPLY CHAIN ENTITIES HAVE INCREASED

NEW PRODUCT INTRODUCTIONS HAVE BEEN MORE FREQUENT

PRODUCTS AND SERVICES HAVE BECOME LESS STANDARD

THE NUMBER OF ENTITIES IN THE SUPPLY CHAIN HAS INCREASED

THE RELATIONSHIPS BETWEEN SUPPLY CHAIN ENTITIES HAVE BECOME LESS TRANSPARENT
Complexity in Action

- Smartphone supply chain
  - Components sourced worldwide
  - Converge in China or India for assembly
  - Multiple opportunities for breaches
Growing Concern: Internet of Things (IoT)

- More than 6 billion things in IoT
- 5+ million things connected every day
- 20 billion by 2020
- Huge multiplier effect on supply chain security risk
- A hack to just one WiFi-connected IoT device can provide access to multiple devices on one network
  - In 2015, 2 researchers were able to wirelessly take control of a Jeep Grand Cherokee, resulting in a recall of 1.4 million vehicles.
Supply Chain Risk Management – Still Not a Priority

• 90% of firms do not formally quantify risk when sourcing production

• Study by Risk and Insurance magazine: 0 rated their company as “highly effective” at SCRM

• Typical supply chain manager estimates only 25% of company’s end-to-end supply chain is being assessed in any way for risk

• 47% have NO back-up plan if disaster strikes
Countermeasures

• 2011 National Defense Authorization Act:
  • Exclude vendors without a hearing if they believe that vendors pose a security risk.
  • Requires supply chain risk to be included as an evaluation factor in the procurement process.
  • Needs to be more proactive:
    • Average of 146 days* to detect breaches - means a supply chain could be breached but still in operation before the government identifies vulnerability and excludes it from its supply chain.

Countermeasures

2014 - Cyber Supply Chain Management and Transparency Act introduced

• Would mandate that security contractors provide a bill of all materials used in their products, including open-source software, and that each contractor demonstrate strong cybersecurity practices

• Act never passed – opposition from contractors and tech companies
Countermeasures

NIST Cybersecurity Framework & best practices white paper

• Recommendations are nonbinding
• Bottom line: “Federal policy surrounding supply chain security is lacking, particularly as it pertains to the private sector and its civilian consumers.”*

Countermeasures

• One potential solution: The Open Group Trusted Technology Forum (OTTF) - standards relating to supply chain security guidelines for tech companies, called the O-TTPS V1.1

• OTTF also offers a certification program – suppliers & distributors can signal to business partners and consumers that their products have met certain safety standards

• OTTF certification could be a way for users to manage risk
What Are Industry Sectors Doing?

Pharma

- Serialization – track and trace of drugs throughout the supply chain, from manufacture to dispensing
- Global regulations require digital chain of custody – drug pedigree
- Purpose: Combat counterfeits, adulteration, diversion, etc.

Pharma Serialization Database

Risk Based Verifications

Authentication only when Recall, Returns, Suspect Activity Reported

Authentication for Recall, Return, Suspect Activity

Authentication for Recall, Resale, Return, Suspect Activity

TH = Transaction History
TI = Transaction Information
TS = Transaction Statement
Other Pharma Collaborative Efforts

• Pharma coalitions – anti-theft
  • Pharma Cargo Security Coalition
  • Pharmaceutical Security Institute
  • National Biopharmaceutical Security Council
  • Pharmaceutical Security Council

• Results:
  • 2009 – 47 large-scale thefts; average loss each incident - $4.2 M
  • 2013 – 23 incidents; average loss - $228,000
New Thinking: What’s Being Done?

The Plug-and-Play Supply Chain
Reducing Complexity: Time for change

42% of respondents will reduce their number of supply chains over next 3-5 years

32%\(^1\) of respondents operate more than 10 different supply chains

\(^1\) DHL survey data point: 350 global respondents
One-off Supply Chains are Unsustainable

High cost

Cumbersome/ lacks agility

Risky: Complexity leads to security risks, quality & performance failures

69% of companies are pursuing standardization

1) DHL survey data point: 350 global respondents
The Plug-and-Play Supply Chain

What is it?

• Core, standardized, easily replicated solutions, augmented by standardized bolt-ons

• Two key building blocks:
  1. Smart segmentation
  2. Standardization

Core solutions should satisfy 70-80% of the requirements in a market segment.
Building Block 1: Smart Segmentation

• Most think of segmentation as a profitability strategy
• Designing & operating the supply chain by understanding specific performance characteristics of products, channels, manufacturing and supply capabilities & service models
• Purpose: To create the most profitable supply chain – total cost to serve
• Why not put segmentation to another use: Supply chain risk management?
  • E.g., Supplier segmentation: Segment by impact (financial, mission, etc.), recovery time and cost, probability, ability to affect, etc.
• Apply the same type of segmentation to security & risk
• The difference is data analytics
• Make smarter decisions
Profit Contribution Example

• Analytics-driven insight
• Segment customer delivery locations into profit contribution groups
• This example - analysis reveals that less than 5% of customer delivery locations represent 80%
• Conversely, 95 percent of customer delivery locations are only marginally profitable

Risk management application – same approach
Building Block 2: Supply Chain Standardization

DHL survey:

• 69% of companies are pursuing supply chain standardization – the plug-and-play approach
• Only 16% are well along
• Key emphasis: Create repeatable supply chain components and solutions

• Standardization reduces risk
Standardized Solutions Library

• “It was taking all of our effort to manage the existing complexity in our business. We had to find a better way. Our biggest challenge was the fact that we were solving the same problem over and over again and not creating an institutional corporate memory of best practices so they could be replicated.”

  – Gary Keatings, DHL

• WHAT DHL did
  • Began building databases and libraries of customer-facing best practices
  • Stopped reinventing the wheel over and over again

Core solutions should satisfy 70-80% of the requirements
Building the Solution

• Now – for a new customer or project, DHL follows a 2 step process

• Step 1:
  • Capture and profile the supply chain
  • Match it against database of supply chains DHL already created & executed
  • Get a quantitative score – e.g., 85% match to these three other customer supply chains – traits, assets, personnel, systems, processes, geography, etc.
  • Build the **CORE STANDARDIZED SOLUTION** – the 80% new supply chain based on standardized modules
  • Eliminate as many unique variants as possible
Building the Solution

• STEP 2:
  • Figure out what the last 10% - 15% percent plug-ins should be
  • Make plug-ins as standardized as possible
  • Solve for any really unique challenges on top of that – e.g., the last 5%

• Tangible benefits
  • Example: Implementation start-up lead time and cost decreased by as much as 70%

Plug-and-play approach could be adapted to supply chain security & risk management
Cisco – Plug-and-Play at Work

• Cisco update: A 10+-year journey

• Holistic SCRM framework – cross organizational – entire ecosystem
  o 6 major risk categories, 25 subcategories
  o Mapped onto visual display
  o X axis – probability/likelihood
  o Y axis – mitigation difficulty...includes resources required ($$ and people) to mitigate and level of control over the event
  o Real-time visibility into production of suppliers

• Guiding principle: Continuity of supply; mitigate vulnerabilities before a disruption

• Mitigation efforts prioritized by revenue

• Four primary risk management strategies:
  o Incident management
  o Supplier business continuity planning
  o Manufacturing and test resilience
  o Product resilience
Cisco – Security Domains - Suppliers

11 security domains; 180 requirements. Some requirements applicable across the board — e.g., security governance or personnel security. Others customized to the product, service or site.

1. Security governance
2. Security in manufacturing & operations
3. Asset management – securing IT, manufacturing assets throughout lifecycle
4. Security incident management
5. Security service management – e.g., continuity programs
6. Security in logistics & storage
7. Physical & environmental security – facilities, etc.
8. Personnel security
9. Information protection
10. Security engineering & architecture – security requirements followed in design, development, testing and rollout
11. 3rd tier partner security – information security controls at downstream suppliers

- Value at risk
- Time to recover
- Control tower visibility – real time
Cisco Supply Chain Security Ecosystem

- Holistic – entire 3rd party ecosystem
- End-to-end
- Including end of life
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
Summing Up: Underlying Basics

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

More Work To Do

• Supply chain security risk is escalating exponentially
  • Physical and virtual/cyber threats
• Few organizations are mature in managing SC risk, especially with suppliers
• Resiliency is even tougher to achieve
• Best practices & frameworks are out there
• Action is imperative
Questions?

CONTACT INFORMATION: lisa@lharringtongroup.com • lharring@umd.edu • Phone: 410.725.6198