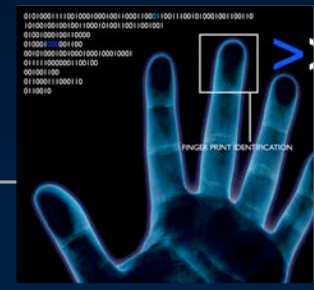
U.S. DEPARTMENT OF ENERGY | Office of the Chief Information Officer

The Wolf in Sheep's Clothing

Sharing the Knowledge of Supply Chain Risk



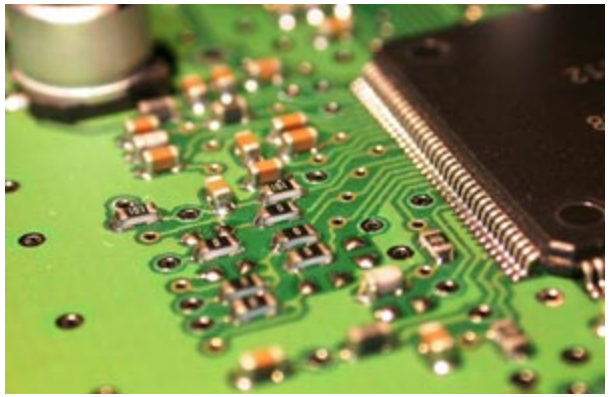
In January 2012, the Director of National Intelligence identified the vulnerabilities associated with the information and communications technology (ICT) supply chain as one of the greatest strategic cyber threat challenges the country faces.

“IT supply chain integrity issues . . . are growing more complex as IT systems are assembled from a large number of geographically diverse providers, and, now of mainstream concern to enterprise IT. This has significant implications for businesses, governments and individuals moving forward in a world where the integrity of the IT supply chain is no longer completely trustable, and where all layers of the IT stack will be targeted for supply chain compromise.”

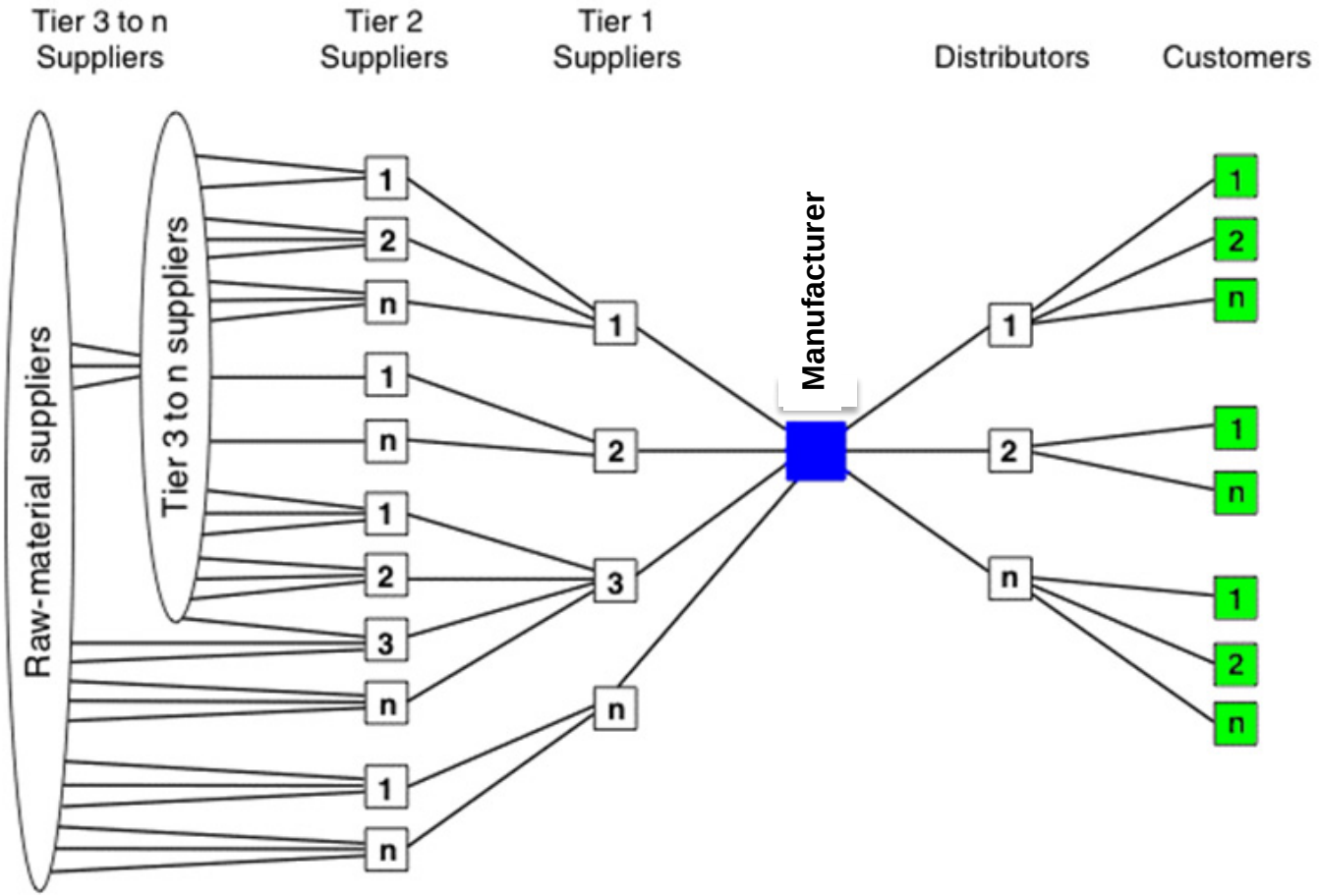
Ray Valdes
Research Vice President, Gartner, Inc.

Information and Communications Technology

- **ICT covers any product that stores, retrieves, manipulates, transmits, or receives information electronically in a digital form,** including
  - **The traditional computer-based technologies** and
  - The fast-growing range of **digital communication technologies**
- ICTs enable organizations
  - To produce, access, adapt and apply information
    - In greater amounts,
    - More rapidly,
    - At reduced costs,
  - And offer opportunities for enhancing business and economic viability.



Supply Chain Basics



Source: National Research Council Staff (2000). *Surviving supply chain integration: strategies for small manufacturers*. Washington, DC: National Academies Press.

The Crux of the Problem

The ICT supply chain has become more complex, globally distributed, and unpredictable.

- Rapid change provides the opportunity to introduce compromises.
- Conglomeration of components and subsystems are procured from a large number of individual providers.
- Outsourcing of design and manufacturing is increasing.
- Tiers and systems of suppliers are becoming more complex.
- Supply chain risks are not widely understood.
- SCRM is generally an unknown issue for professionals in the system lifecycle.

Federal Focus on ICT SCRM

- Reliance on a global supply chain introduces multiple risks to Federal information systems and can adversely affect an Agency's ability to effectively carry out its mission.
- ICT supply chain-related threats can be introduced anywhere in the system development life cycle.
- Organizations are often not aware of where components originate or how they were put together.
- Compromise of the ICT supply chain can degrade the confidentiality, integrity, and availability of networks, IT-enabled equipment, and data.

Things are not what they seem

- ICT SCRM involves five different challenges
  - **Malicious logic** in hardware or software
  - **Counterfeit** hardware or software
  - **Failure or disruption** of a critical product or service
  - **Malicious or unqualified** supplier
  - Installation of **unintentional vulnerabilities**

ICT Supply Chain Concerns

- Resilience
- Integrity
  - There is an ongoing need for stronger and more resilient information systems.
  - Supply chain integrity is the requirement that *the system performs its intended function in an unimpaired manner, free from deliberate or inadvertent manipulation.*
  - Supply chain integrity will be identified among the top three security-related concerns of IT leaders by 2017, according to 2012 research by Gartner.

Risk in the Supply Chain

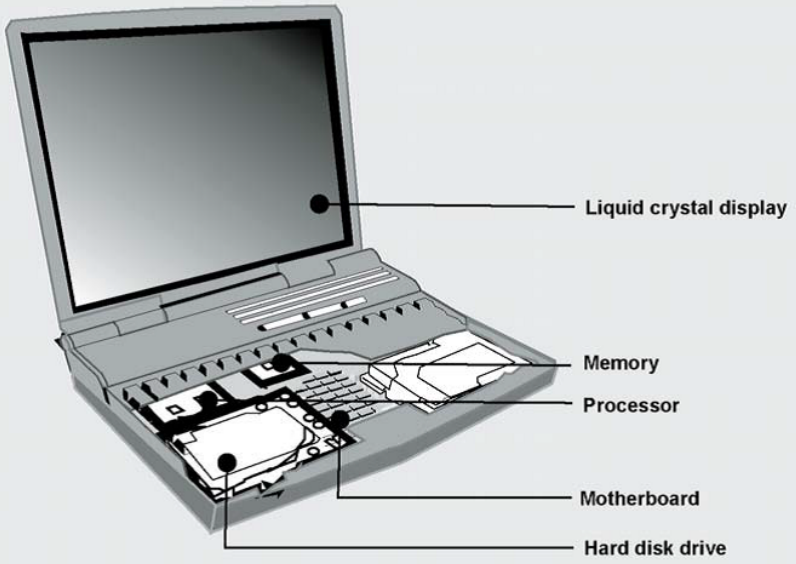
- Supply chain risk stems from multiple factors:
  - Growth in dependencies on technology,
  - Growth in dependency on commercial software,
  - Supply chain globalization,
  - Lack of insight into processes under which products are made,
  - Inadequate procurement practices, and
  - Fragmented decision-making.

- Gartner predicts that by 2016, a publicly disclosed ICT supply-chain-integrity-related incident, costing millions in remediation and data loss, will affect at least 25 percent of the top 2,000 public companies in the world.

Supply Chain Globalization

- There's nothing new about globalization
  - Sourcing, manufacturing, transporting, and distributing products to other countries
  - Predates the Internet by at least 40 years
- The world is "flatter," and supply chains are longer.
- Product development and manufacture is internationally distributed.
- The key concern is to manage risks to the integrity of the system components as they move through their lifecycles.

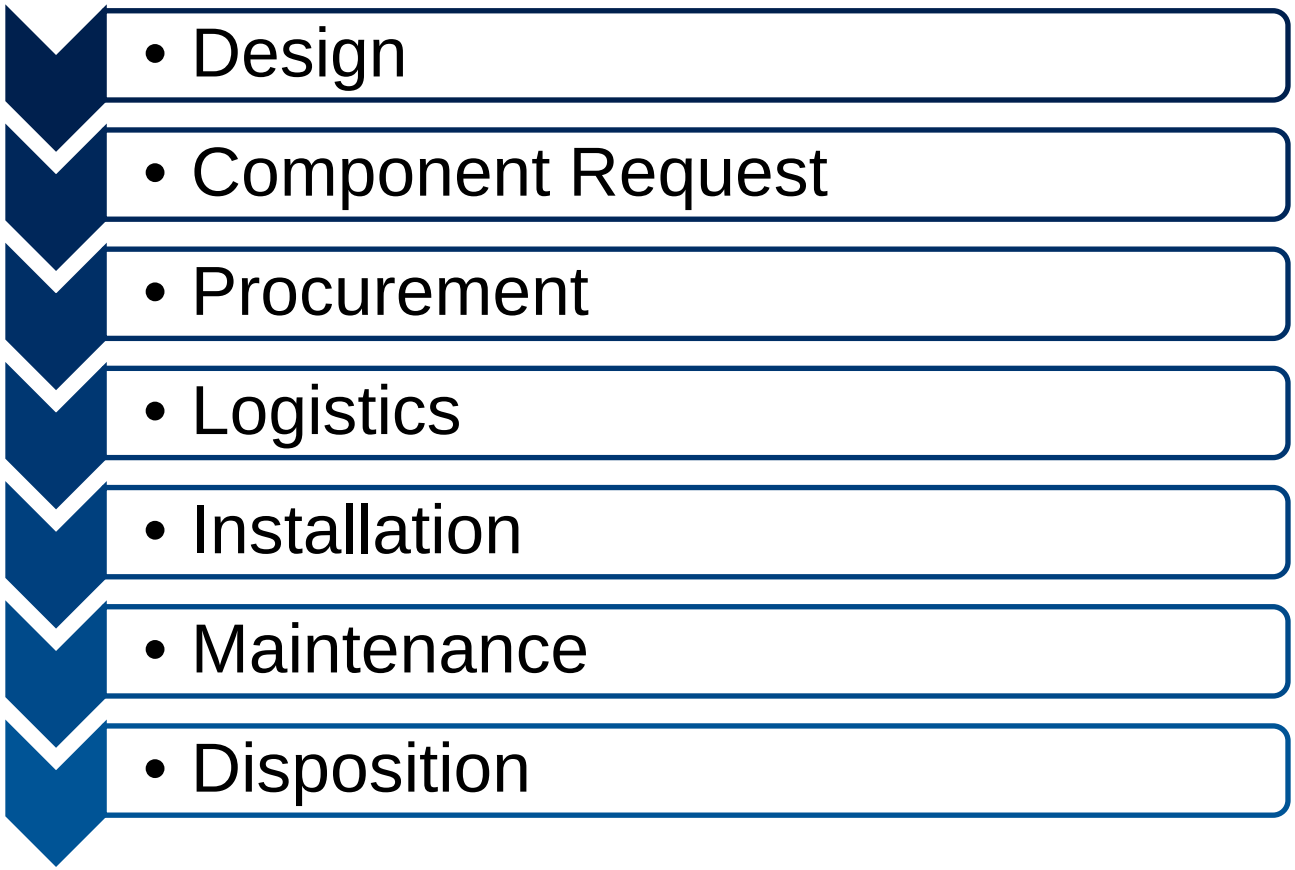
Laptop Component Sources



Component	Location of facilities potentially used by suppliers
Liquid crystal display	China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan
Memory	China, Israel, Italy, Japan, Malaysia, Philippines, Puerto Rico, Singapore, South Korea, Taiwan, United States
Processor	Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam
Motherboard	Taiwan
Hard disk drive	China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States

Source: GAO analysis of public information.

The Internal “Supply Chain”



Things can go wrong here, too!

Everyone shares the problem

Anyone who has one of these:

And one of these:

Or one of these:

Poses a
supply chain risk.

Staff Responsibility Training

- **Purpose: Increase the capabilities of employees to effectively support a secure ICT supply chain**
- **Outcomes:**
  - Understand responsibility and accountability for the protection of ICT resources
  - Understand the impacts of supply chain issues to the security of information assets
  - Become familiar with job functions and related skills that relate to supply chain risk
  - Demonstrate due diligence in carrying out SCRM responsibilities

U.S. DEPARTMENT OF ENERGY

Can we train to manage supply chain risk?

Challenge of Training about Risk

- People consider two key elements in understanding the risk of a “bad thing happening.”
  - Threat likelihood and severity
  - Their ability to control the risk
- We’ve spent nearly three decades telling people the facts about cybersecurity risks and waiting for them to “get it.”
- If people aren’t acting to control risk, then
  - Either they don’t think the issue is significantly dangerous or
  - They lack confidence in their ability to manage it.

SCRM Training Challenges

- Low acceptance of the concept of supply chain risk
- Immaturity of the content area
- More than a cybersecurity or IT issue
- Wide range of potential students
- Minimal understanding of the key competencies required for
  - supply chain management roles,
  - specific job qualifications,
  - methods for developing future talent and leaders, and
  - the ability to efficiently source specific skill sets.
- No clear integration with other training
- Unknown measurable outcomes
- Lack of top management understanding
- Training “boredom”
- Inability or unwillingness to share information
- Not an issue users can address in the workplace
- Legal ramifications
- Lack of training for new mindsets and skills

Solutions, Anyone?

- DoD, DHS, DOJ, and DOE are building ICT SCRM training and awareness programs.
- But don't wait . . .
  - Do the research
  - Understand the problem
  - Identify the players
  - Start simple
  - **Add SCRM to awareness and training efforts**

Great Resources:

CNSS 505
NIST IR 7622
NIST SP 800-16
NIST SP 800-37
NIST SP 800-39
NIST SP 800-50
NIST SP 800-53, Rev 4

NIST says: A strong supply chain risk mitigation strategy cannot be put in place without **significant attention given to training** personnel on supply chain policy, procedures, and applicable management, operational, and technical controls and practices.

U.S. DEPARTMENT OF ENERGY

Susan Farrand

SCRM Program Manager

US Department of Energy

susan.farrand@hq.doe.gov

202-586-2514

U.S. DEPARTMENT OF ENERGY

Backup Slides

The Threat in Hiding

Basic Definitions from CNSSI 4009

- **Risk:** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.
- **Threat:** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
- **Vulnerability:** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Risk Management Basics

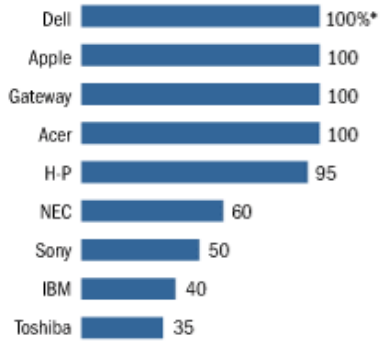
- Risk is any event, practice, process, activity, etc. that has an uncertain outcome.
- It is any threat to the achievement of mission objectives.
- Risk Management is the
  - Identification,
  - Assessment, and
  - Mitigation

  of any action with real or potential adverse impacts.

All Over the Map

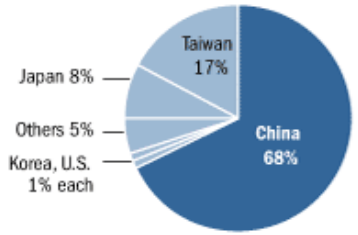
When a U.S. customer orders an H-P Pavilion laptop, the request travels all the way to China in just days. A look at the process, and China's increasing role not just as manufacturer, but supplier of more sophisticated laptop parts

Outsourcing ratio for world's top laptop PC brands, 2004:



*Dell takes care of final assembly in its factories.
Source: Merrill Lynch

World-wide laptop PC production by country, 2005:



Source: IDC

Filling the order

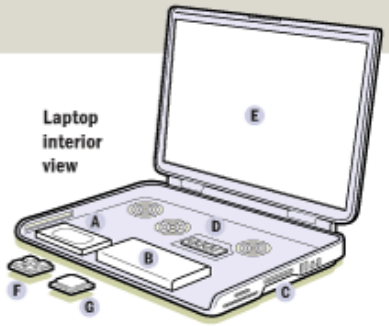
1. **Order** placed online in the U.S.
2. **Validated** order transmitted to Taiwanese-owned Quanta plant in Shanghai
3. **Laptop assembled** from parts from China and all over the world
4. **Computer shipments** consolidated at Shanghai airport and flown freight to the U.S.
5. **Individual laptops** sent to customers

H-P Pavilion zd8000 laptop computer

Putting it together

A	**Hard-disk drives**	Japan, China, Singapore, U.S.
B	**Power supplies**	China
C	**Magnesium casings**	China
D	**Memory chips**	S. Korea, Taiwan, U.S., Germany
E	**Liquid-crystal display**	S. Korea, Taiwan, Japan, China
F	**Microprocessors**	United States
G	**Graphics processors**	Designed in U.S., Canada; made in Taiwan

Note: List does not include every country that manufactures a given part
Sources: Hewlett-Packard; WSJ research



Source: Wall Street Journal, June 2005

Executive Order 13626

- February 12, 2013
- Purposes
  - Enhance the security and resilience of the Nation's critical infrastructure and
  - Maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties
- The Cybersecurity Framework
  - A set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks
  - Incorporates voluntary consensus standards and industry best practices to the fullest extent possible.
  - Consistent with voluntary international standards