



Cyber Supply Chain Assurance

Putting the challenge in context: Why security platforms and architectures of participation are the foundations of a winning strategy

Hart Rossman

June 2010

Energy | Environment | National Security | Health | Critical Infrastructure



A Recognized Systemic Risk




It's a national security imperative in a global economy that we have confidence in the supply chains of integrated systems and the integrity of the people, processes and technology that comprise them.



The Threat Is Real

Vendor FAIL - Certified Pre-Owned (CPO)

How vendors screw up their own products and leave YOU holding the virtual bag

 For reasons unknown, vendors occasionally fail to maintain quality control over the media they ship. Whether it is CD-ROM, DVD, USB or some other form of media, it may contain viruses, trojans or even drug-runner music. When this happens, the software you receive obviously can't be trusted in any fashion, and installing software from already compromised media immediately puts your system's integrity in question. This page serves to keep a record of such incidents and remind vendors that shipping "pre-owned" software is deplorable. This list is designed to capture consumer related exposures, specifically malware or other items of interest. This list will not include incidents of vendors shipping vulnerable software as that list would be **extensive**. In addition, it will not track targeted malware attacks against specific targets, such as the "Farewell Dossier". For an interesting historical perspective of such incidents until 1996, consult **McDonald's list**. Some of these incidents are integrated in the CPO list depending on the information available.

When	Who Shipped	What Media	With What
2009-01-02	Element	9-Inch Digital Photo Frame	Unknown
2008-12-29	Samsung	SPP-85H 8-Inch Digital Photo Frame	Sality Worm
2008-12-28	Mercury	Mercury 1.5" Digital Photo Frame	DPFMate.exe and FEnCodeUnicode.dll
2008-10-27	Teq AV	Wireless AV System USB Key	Multiple (W32.Perlovga family)
2008-10-15	Unspecified	Credit Card Terminal	Physical bug to steal credit card

Source: <http://attrition.org/errata/cpo/>



Source: <http://www.andovercrg.com/services/cisco-counterfeit-wic-1dsu-t1.shtml>

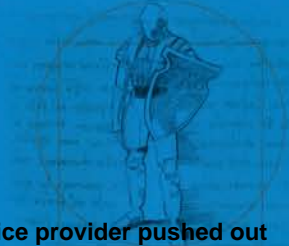
“At a meeting in January, Alex Allan, chairman of the Joint Intelligence Committee, told the Home Secretary that while BT had taken steps to secure its network, "we believe that the mitigating measures are not effective against deliberate attack by China", the *Sunday Times* [reports](#).”

“Huawei, led by former People's Liberation Army (PLA) research chief Ren Zhengfei, is a major supplier to BT's ongoing multi-billion-pound 21CN network upgrade. It will see all voice and data traffic carried by the same packet-switched equipment. In 2005 the Chinese firm won contracts to provide access nodes and optical equipment for the core of the new network.”

Source: 30 March 2009 http://www.theregister.co.uk/2009/03/30/huawei_threat/



The Threat Is Real



July 14, 2009

“A BlackBerry update that a United Arab Emirates service provider pushed out to its customers contains U.S.-made spyware that would allow the company or others to siphon and read their e-mail and text messages, according to a researcher who examined it.

The update was billed as a “performance-enhancement patch” by the UAE-based phone and internet service provider [Etisalat](#), which issued the patch to its 100,000 subscribers.

The patch only drew attention after numerous users complained that it drained their BlackBerry battery and slowed performance, according to local publication [ITP](#).”

Source: <http://www.wired.com/threatlevel/2009/07/blackberry-spies/>

July 16, 2009

“German buyers of the Toshiba TG01 smartphone got more than they bargained for when O2 shipped units infected with unknown malware. The German arm of O2 has been forced to suspend sales of the Toshiba TG01 smartphone after it discovered that stocks were infected with malware. As reported over on The Register , the mobile carrier has confirmed that sales of the Toshiba TG01 handset have ceased as a result of the discovery, which saw the company alerted to an unnamed virus hiding within the ‘phone. So far, O2 has been cagey on the details: it’s not yet known whether the virus was one capable of executing on the TG01’s Windows Mobile 6.1 operating system, or simply a standard bit of malware which was stored on the memory awaiting the first time the device is connected to a suitable desktop or laptop to execute.”

Source: <http://tech4review.com/2009/07/16/o2-ships-malware-on-toshiba-handsets/>

July 29, 2009

“Windows 7 has yet to even be released officially to the general public, and already the dodgy folk on the [Internet](#) have fully cracked and activated the Ultimate version, with help from a leaked Lenovo OEM DVD .ISO file.

The news comes from various Chinese forums who state that you can already pass Windows Genuine Advantage validation offline, OEM style.

The leaked .ISO was originally posted on a Chinese forum, which was then downloaded in order for people to get hold of the boot.wim, and in turn retrieving the OEM-SLP key, plus the OEM activation certificate. Microsoft uses the same digitally signed OEM certificate, which has an .xrm-ms extension, as that in Windows Vista. Another point to note is that the key is a master one, which can be used to activate other OEM branded installations, like ones from Dell, HP or indeed Lenovo.

This is quite concerning; as mentioned, Windows 7 has yet to even be released, and it can be fully activated. This demonstrates the risk such a huge company as Microsoft takes when distributing a product as significant as an [operating system](#), but this was essentially inevitable, regardless. It’s interesting that a product can be pirated and activated before it’s properly released to customers.”

Source: <http://www.neowin.net/news/main/09/07/29/windows-7-ultimate-cracked-and-activated-with-oem-master-key>

Yet Visibility Is Limited



Electronic Supply Chain Association Study (2005):

- Visibility into closest trading partner is good
- Drops off significantly after that
- 10% didn't know whether they had visibility or not into Tier 1 and 2!

- Overall, ESCA study – 55% of outsourcers and 45% of service providers have limited visibility into 2nd tier trading partners

Office of Technology Evaluation (OTE)



MISSION:

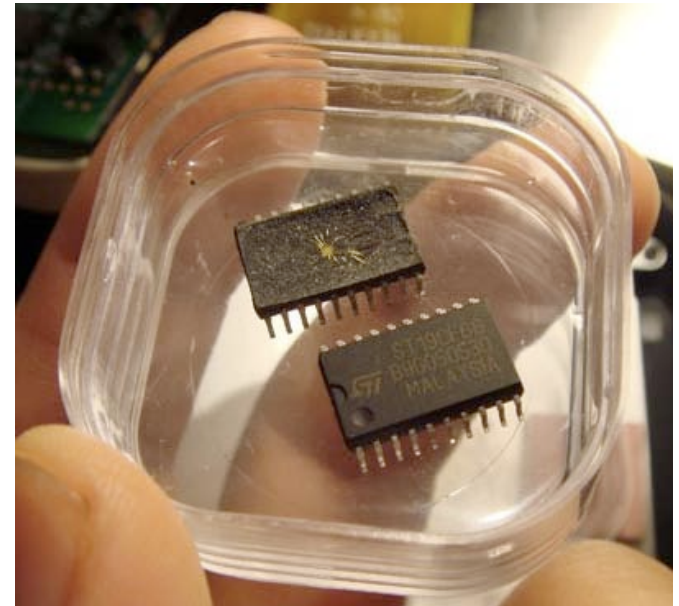
OTE is the focal point within BIS for assessing:

- The effectiveness of export controls
- The capabilities of the U.S. industrial base to support the national defense

Counterfeit Electronics Study -Goals



- Assess the impact of counterfeit electronics on U.S. supply chain integrity, critical infrastructure, and industrial capabilities
- Recommend best practices mitigate risk to U.S. supply
- Study sponsored by Naval Systems Command with from Semiconductor Association (SIA)



Counterfeit Electronics

-Broad Definition



- An electronic part that is not genuine because:
 - An unauthorized copy
 - Does not conform to original OCM design, model, and/or performance standards
 - Not produced by the OCM or is produced by unauthorized contractors
 - An off-specification, defective, or used OCM product sold as "new" or working
 - Has incorrect or false markings and/or documentation

Counterfeit Electronics Study

-OTE surveys distributed



- 5 separate but related surveys targeting:
 - Microchip & discrete electronic manufacturers – 106
 - Electronic board producers/assemblers – 37
 - Distributors and brokers of electronic parts – 144
 - Prime contractors and subcontractors – 147
 - DOD arsenals, depots, and DLA – 64
- 498 total survey participants



Counterfeit Electronics Study

-Themes



- Lack of dialogue between all parties
- Insufficient chain of accountability
- Assumption that others in the supply chain are testing the product
- Record keeping is non-existent
- No one knows who to contact in the Federal government
- There needs to be stricter testing protocols and monitoring
- Most DOD organizations do not have policies in place to prevent counterfeit parts from infiltrating their supply chain
- No type of company or organization has been untouched by counterfeit electronic parts

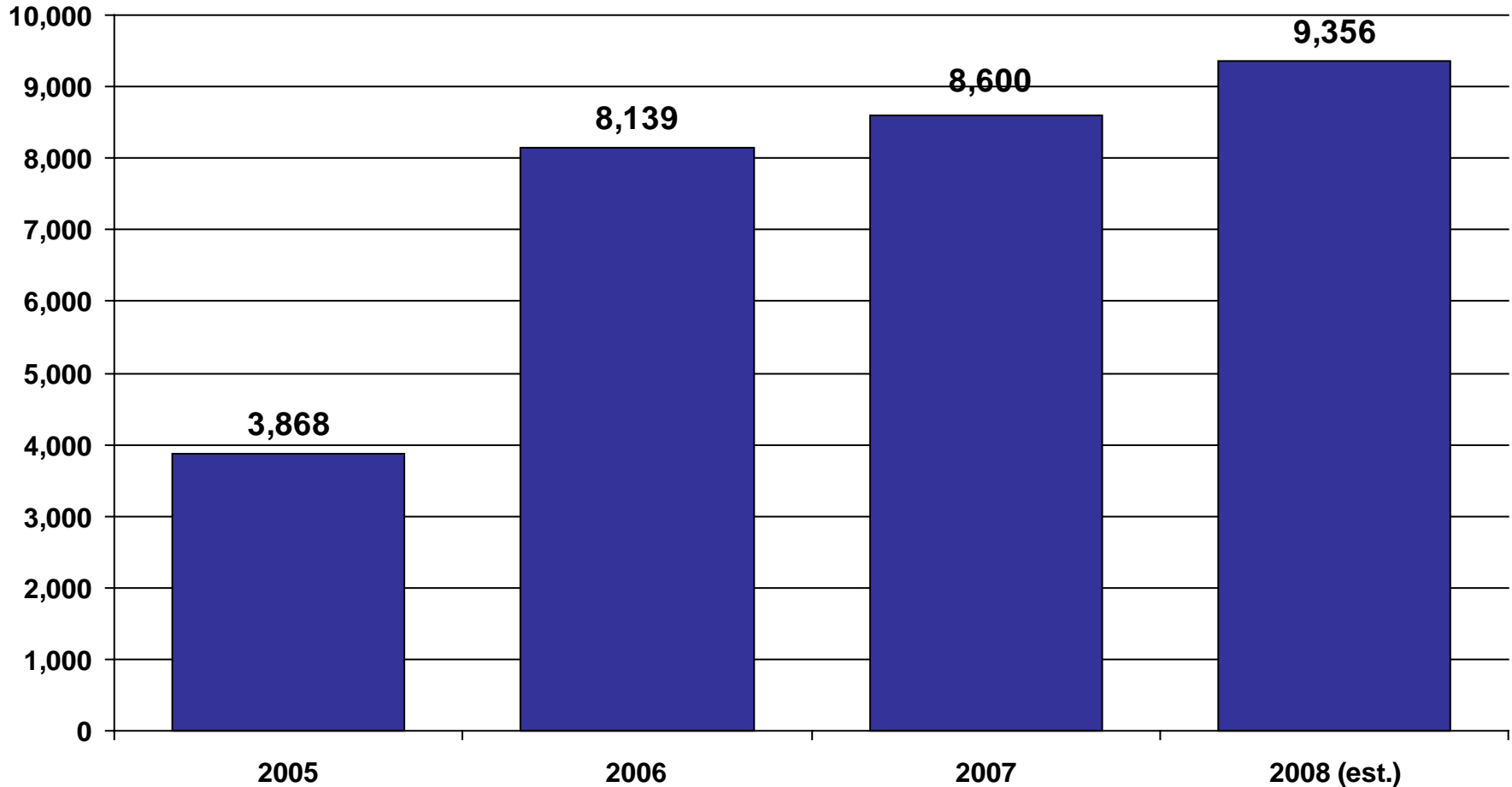
Everyone must work together to solve the problem.

BIS Counterfeit Electronics Survey – Preliminary Data



Type of Company/Organization		Encountered Counterfeits	No Counterfeit Incidents	Total
OCMs	Discrete Electronic Components	18	21	39
	Microcircuits	24	20	44
Distributors	Authorized Distributors	10	35	45
	Independent Distributors	36	8	44
	Brokers	8	1	9
Board Assemblers		11	21	32
Prime/Sub Contractors		31	90	121
Department of Defense	DLA Organizations	3	16	19
	Non-DLA Organizations	11	23	34
Total		152	235	387

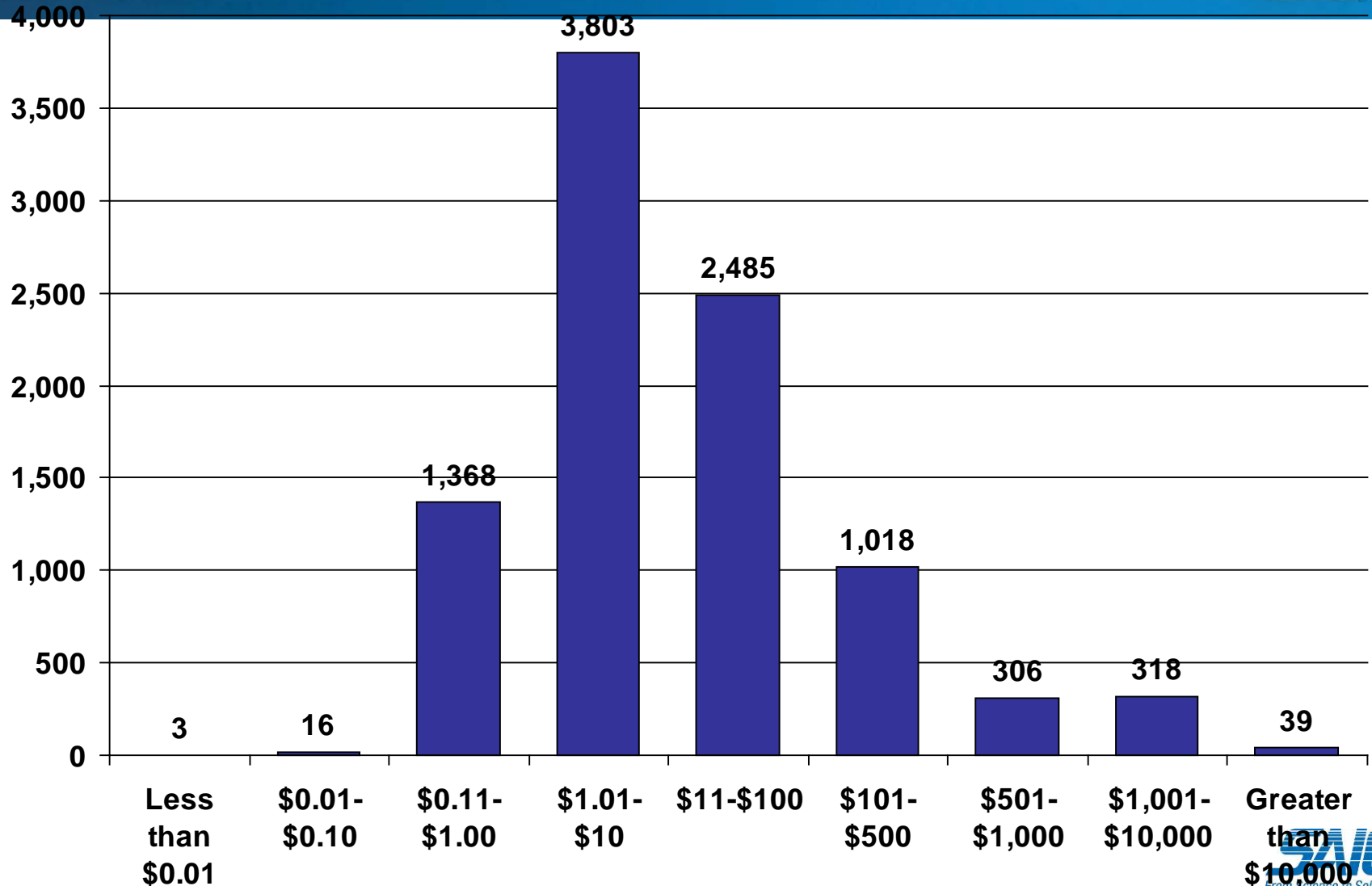
Total Counterfeit Incidents: OCMs, Distributors, Board Assemblers, Prime/Sub Contractors 2005 - 2008



Energy | Environment | National Security | Health | Critical Infrastructure



Counterfeit Incidents by Product Resale Value: Overall (2008 est.)



Energy | Environment | National Security | Health | Critical Infrastructure



Cyber-Supply Chain Assurance Reference Model



- Collaborative initiative between RH Smith School Of Business Supply Chain Management Center & SAIC to create a **research-based assurance model** that fuses the Cyber Security and Supply Chain Risk Management (SCRM) fields for better command and control over critical information infrastructure.
- Our research has focused on addressing **CNCI's Initiative 11 SCRM challenges**: the need to overcome functional silos in a Cyber-Supply Chain & to establish joint risk governance responsibilities and a shared code of practices across key actors to meet real-world challenges.
- New federal purchasing guidelines are starting to **contractually specify vendor requirements for SCRM**.
- Our assurance model seeks to **help firms gain visibility over end to end operations** establish more collaborative and robust business ecosystems with customers, distributors and suppliers on a worldwide basis.

Basis for Model



- Phase 1: Literature Review and Interview Guide Development (October –November 08).
- Phase 2: Conducted interviews with 30 thought leaders in the systems engineering, network management, software/hardware development, human factors and supply chain risk management areas (November 2008–February, 2009).
- Phase 3: Compiled interview results, analyze findings, and prepared a Prototype Cyber-Supply Chain Assurance Reference Model for presentation to a focus group convened by UMD/SAIC of 25 government and industry executives (March, 2009).
- Phase 4: Results of this feedback incorporated into a working paper released in late spring/available at <http://www.saic.com/news/resources.asp> (June, 2009).
- Phase 5: Organizational field studies conducted to validate model. (Fall, 2009)
- Phase 6: Large scale industry survey being developed (Spring/Summer 2010)

(SCRM Book forthcoming :“X_SCM: The New Science Of X-Treme Supply Chain Management” (Routledge, August, 2010)



“The future is already here - it is just unevenly distributed”
– William Gibson

Agenda



- Platforms Versus Applications
- Building a Cyber Supply Chain Assurance Reference Model
- Challenges for the incident response team

Why?



- Globalization of IT hardware and software products being built, delivered, maintained, and upgraded increases risk of supply chain attacks.
- It's a national security imperative in a global economy that we have confidence in the supply chains of integrated systems and the integrity of the people, processes and technology that comprise them.
- As a supplier, it costs you money and impacts your reputation when resolving customer issues arising from supply chain compromise.



- The evolution of Internet technology jargon
 - From: “...the killer app...” → To: “...the platform for innovation...”
- Platform – an evolving system made of interdependent pieces that can be innovated upon₁

MapQuest®

An internet mapping application where anyone can get directions

(1 mashup on the web as of 10/4/07, source: www.programmableweb.com)

Google® Maps

An internet mapping platform where anyone can innovate

(1179 mashups on the web as of 10/4/07, source: www.programmableweb.com)

...and you can get directions there too...

- Evolution of platforms
 - 1990s: Most platforms defined on machines/in the runtime environment
 - 2000s: “Web as platform” (Tim O’Reilly, #1 tenet of Web 2.0²)

MapQuest is a registered trademark of AOL LLC in the U.S. and/or other countries.

Google is a registered trademark of Google Inc. in the U.S. and/or other countries.

1. ***Platform Leadership***, A Gawer & M Cussamano, Harvard Business School Press, 2002
2. ***What Is Web 2.0; Design Patterns and Business Models for the Next Generation of Software***, T. O’Reilly, 9/30/2005, http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what_is_web_2.0.html Energy | Environment | National Security | Health | Critical Infrastructure

Platform Leadership Strategy¹

...the Network Is the Platform...



- **ARCHITECTURE:** Establish and maintain the architecture
 - Widely understood, loosely coupled, modular architecture
 - Ensure the integrity of the platform – security, availability, scalability and performance
- **OPENNESS:** Clean, open interfaces that enable innovators to build complimentary products on the platform
 - ***Openness*** as a key to spawning complementers
 - Platform value is directly proportional to the number of complementers
 - Breadth of innovation/number of complementers directly proportional to degree of openness
- **EVOLUTION:** Platform evolution to stay current
- **TECHNOLOGY:** Technology stack with the necessary and sufficient components to support complimentary product providers
 - Utilitarian components and domain-specific components
 - But don't compete with complementers
- **OUTREACH:** Outreach to establish a rich community of complementers with innovation that is enabled by the platform
- **PROCESSES:** Establish key processes for complementers
- **MARKET LEADERSHIP:** Market leadership in the platform environment

1. **Platform Leadership, A Gawer & M Cussamano, Harvard Business School Press, 2002**

How Big Is It?



Email: 90 trillion – The number of emails sent on the Internet in 2009. 247 billion – Average number of email messages per day. 1.4 billion – The number of email users worldwide. 100 million – New email users since the year before. 81 percent – The percentage of emails that were spam. 92 percent – Peak spam levels late in the year. 24 percent – Increase in spam since last year. 200 billion – The number of spam emails per day (assuming 81 percent are spam)

Photos: 4 billion – Photos hosted by Flickr® (October 2009).

2.5 billion – Photos uploaded each month to Facebook®.

30 billion – At the current rate, the number of photos uploaded to Facebook per year.

Users: 1.73 billion – Internet users worldwide (September 2009).

18% – Increase in Internet users since the previous year.

738,257,230 – Internet users in Asia.

418,029,796 – Internet users in Europe.

252,908,000 – Internet users in North America.

179,031,479 – Internet users in Latin America / Caribbean.

67,371,700 – Internet users in Africa.

57,425,046 – Internet users in the Middle East.

20,970,490 – Internet users in Oceania / Australia.

Video: 1 billion – The total number of videos YouTube® serves in one day.

12.2 billion – Videos viewed per month on YouTube in the US (November 2009).

924 million – Videos viewed per month on Hulu™ in the US (November 2009).

182 – The number of online videos the average Internet user watches in a month (USA).

82% – Percentage of Internet users that view videos online (USA).

39.4% – YouTube online video market share (USA).

81.9% – Percentage of embedded videos on blogs that are YouTube videos.

Malware: 148,000 – New zombie computers created per day

2.6 million – Amount of malicious code threats at the start of 2009

921,143 – The number of new malicious code signatures added by Symantec® in Q4 2009.

Social media: 126 million – The number of blogs on the Internet (as tracked by BlogPulse®).

84% – Percent of social network sites with more women than men.

27.3 million – Number of tweets on Twitter® per day (November, 2009)

57% – Percentage of Twitter's user base located in the United States.

4.25 million – People following @aplusk (Ashton Kutcher, Twitter's most followed user).

350 million – People on Facebook.

50% – Percentage of Facebook users that log in every day.

500,000 – The number of active Facebook applications.

Websites: 234 million – The number of websites as of December 2009

47 million – Added websites in 2009. 81.8 million – .COM domain names at the end of 2009

12.3 million – .NET domain names at the end of 2009

7.8 million – .ORG domain names at the end of 2009

76.3 million – The number of country code top-level domains (e.g. .CN, .UK, .DE, etc.)

187 million – The number of domain names across all top-level domains (October 2009)

8% – The increase in domain names since the year before

Trademark attributions are on slide 24.

Source:

<http://royal.pingdom.com/2010/01/22/internet-2009-in-numbers/>



The Facebook Generation

Source: Facebook.com



The tech:

Facebook's

- Cassandra
- Thrift
- Tornado
- Haystack

Apache Foundation's

- Hadoop
- Hive
- Amazon's Dynamo
- Danga Interactive's Memcached
- Scribe

Some useful stats from a planetary-scale computing platform (Facebook®):

- **Users spend 8 billion minutes online everyday using Facebook**
- **There are some 2 billion pieces of content shared every week on the service**
- **Users upload 2 billion photos each month**
- **There are over 20 billion photos now on Facebook**
- **During peak times, Facebook serves 1.2 million photos a second**
- **Yesterday alone, Facebook served 5 billion API calls**
- **There are 1.2 million users for every engineer at Facebook**
- **Seventy percent of Facebook's more than 300 million users are outside the U.S.**

Mobile devices in America are generating something like 600 billion geospatially tagged transactions per day. Every call, text message, email and data transfer handled by your mobile device creates a transaction with your space-time coordinate (to roughly 60 meters accuracy if there are three cell towers in range), whether you have [GPS](#) [Global Positioning System] or not.

Source: http://jeffjonas.typepad.com/jeff_jonas/2009/08/your-movements-speak-for-themselves-spacetime-travel-data-is-analytic-superfood.html

Cisco CRS-3 System - Capable of shifting up to 322 terabits per second



- Cisco® sees it as the first step on the road to the forthcoming “zettabyte era” (four orders of magnitude up from today's gigabit/gigabyte world), which enables “the entire printed collection of the Library of Congress to be downloaded in just over one second; every man, woman and child in China to make a video call, simultaneously; and every motion picture ever created to be streamed in less than four minutes” read the official release.

Source: <http://www.networkworld.com/news/2010/031110-cisco-shows-off-internet.html>

Cisco is a registered trademark of Cisco Technology, Inc. in the U.S. and/or other countries.

Seemingly Huge Advantages



- “Facebook, for instance, created its Cassandra data store in-house to replace its use of MySQL. According to a presentation by [FaceBook engineer Avinash Lakshman \(PDF document\)](#), Cassandra can write 50GB of data in 0.12 milliseconds, more than 2,500 times faster than MySQL.”

Source: http://static.last.fm/johan/nosql-20090611/cassandra_nosql.pdf

- “Meanwhile BigTable, in conjunction with its sister technology, [Google Inc.’s] MapReduce, processes as much as [20 petabytes of data per day.](#)”

Source: <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9131526>

- “.... the fully denormalized Cassandra dataset weighs in at 3 terabytes and 76 billion columns.” <http://blog.digg.com/?p=966>

Source: blog.digg.com

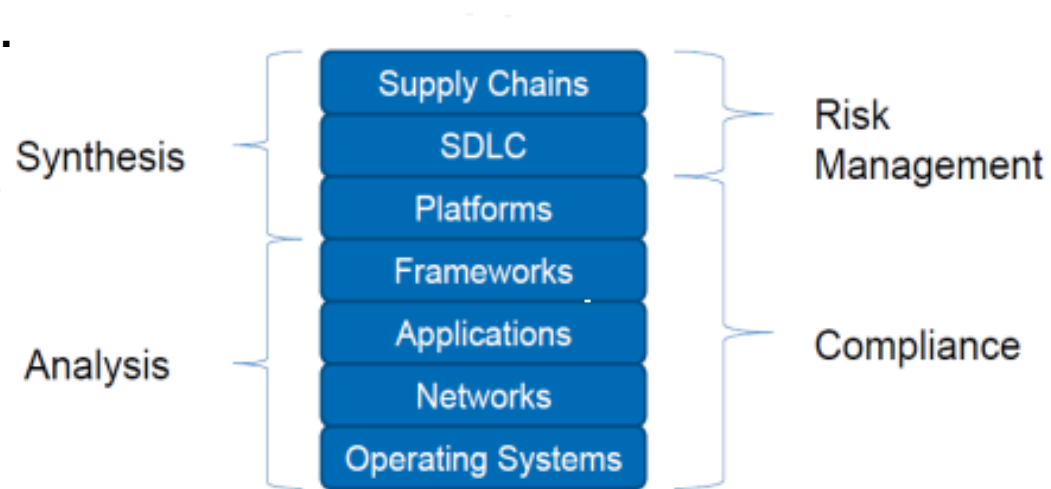
Facebook is a registered trademark of Facebook, Inc. in the U.S. and/or other countries.

The Cyber Security Risk Landscape Is a Convergence Between “Defense in Depth” and “Defense in Breadth”



Enterprise risk management and governance are security motivators.

Planning and acquisition could be considered the beginning of the life cycle, not development.



“In the digital age, sovereignty is demarcated not by territorial frontiers but by supply chains.”

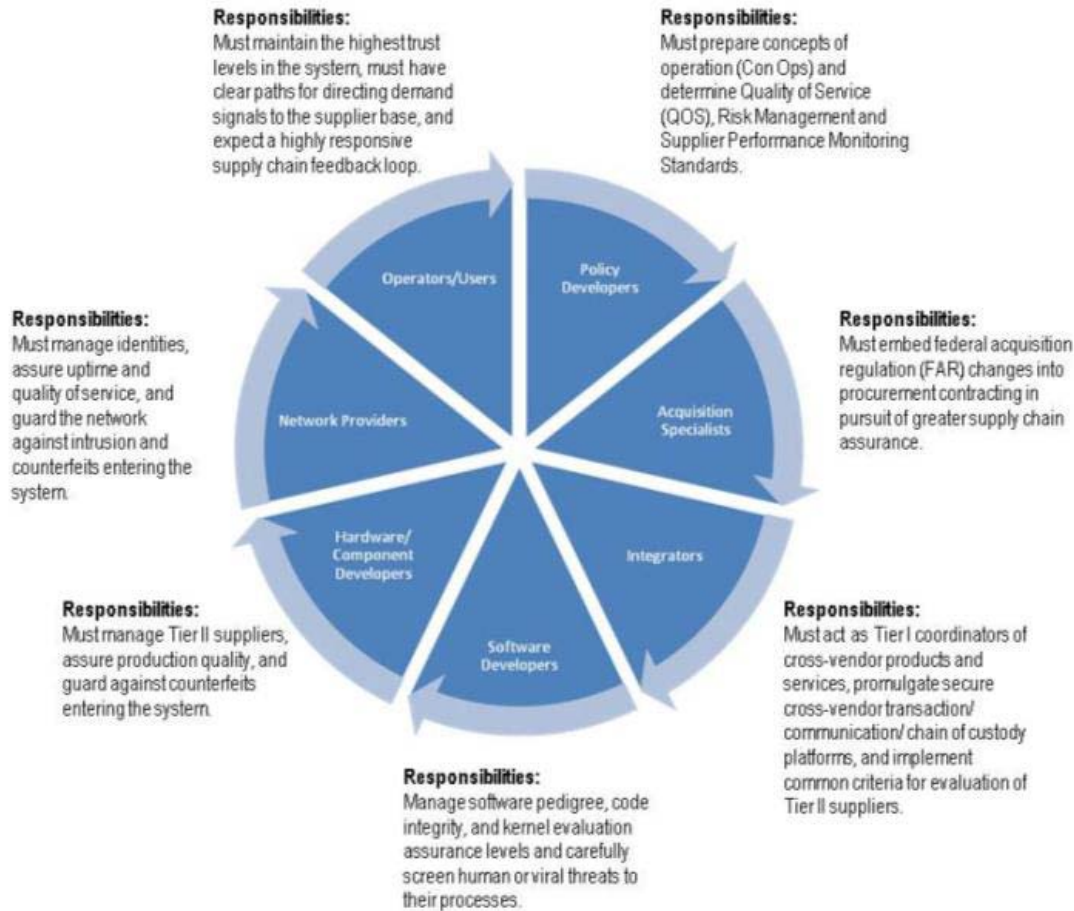
– Dan Geer, CISO, In-Q-Tel, Inc.

Cybersecurity provides focus for:

- Secure hardware, software, and virtual components
- Security in the software development life cycle
- IT supply chain risk management

SDLC = software development life cycle

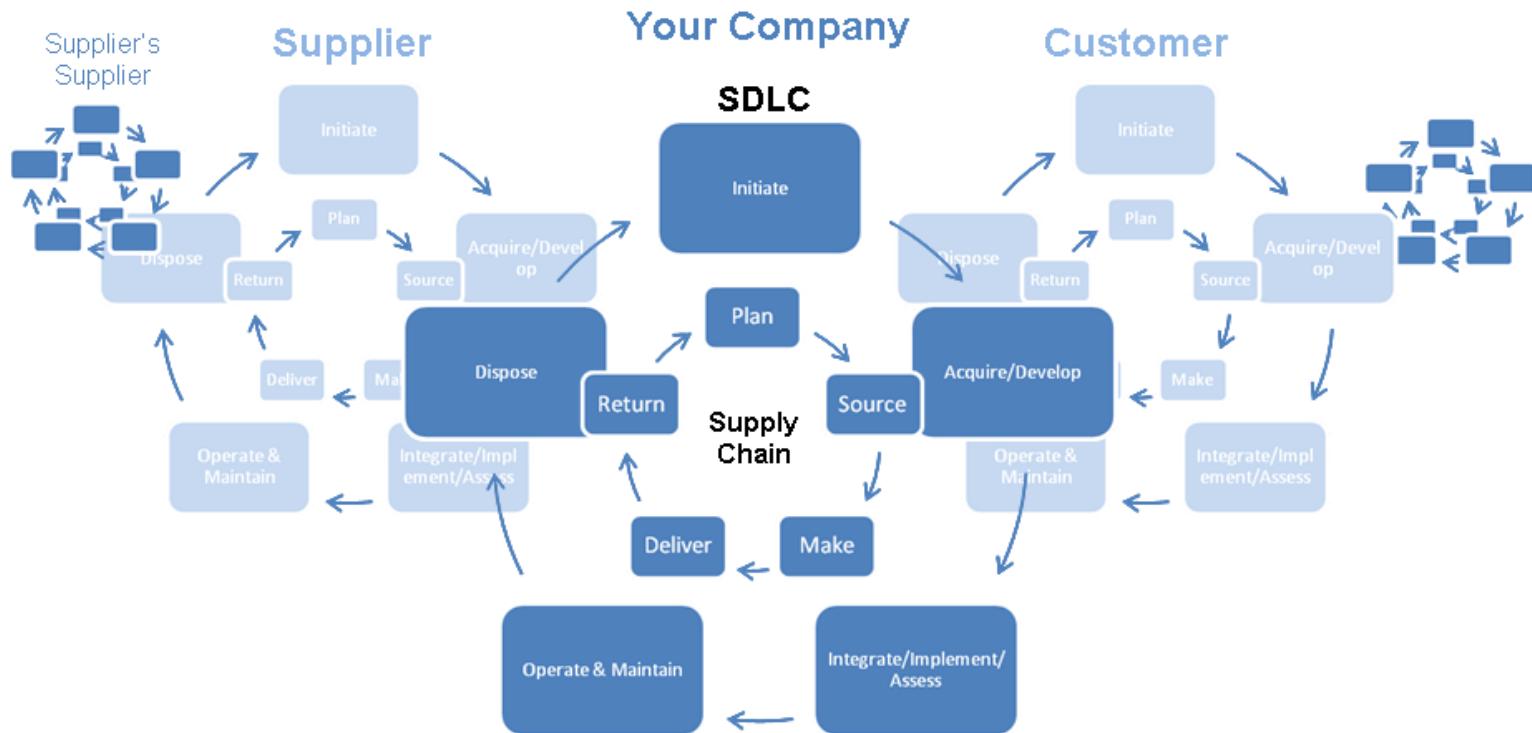
Cyber Supply Chain Ecosystem



System Development Life Cycle and Supply Chain Ecosystem



Emphasis is on the product of the inter-relationships between software development life cycles (SDLCs) across the supply chain



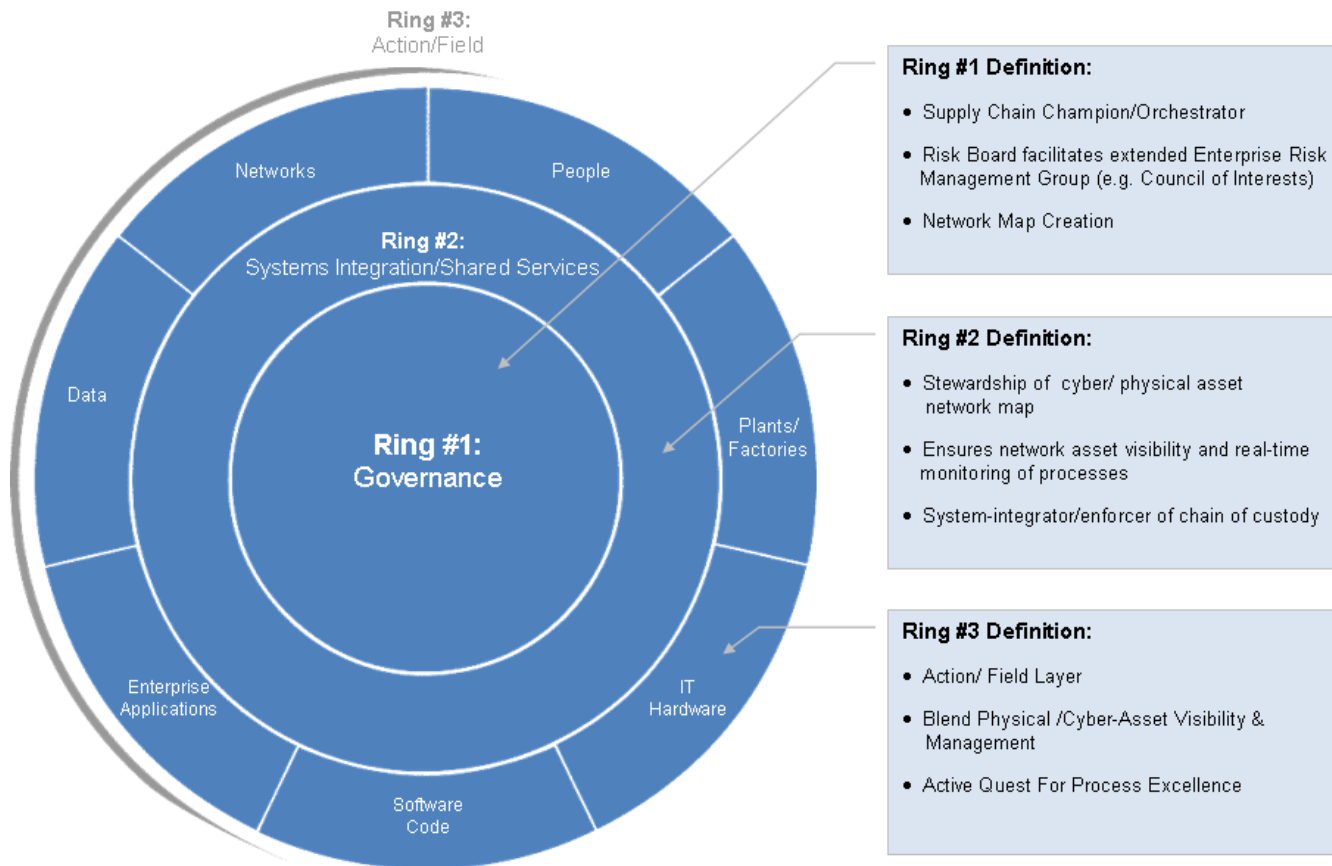
Your organization is not likely the final terminus, therefore assurance mechanisms introduced to your supply chain must be forward-integrated into your customer's (and their customer's) environment.



Cyber Supply Chain Assurance Model



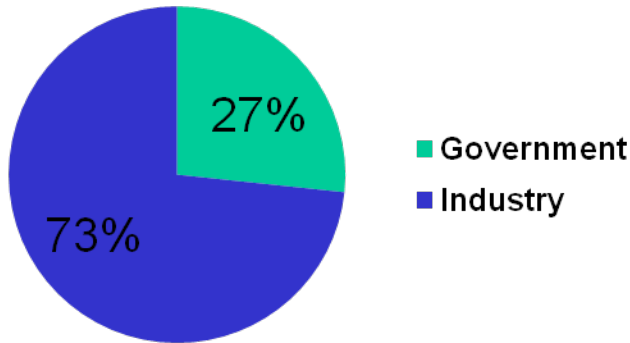
Assurance Model



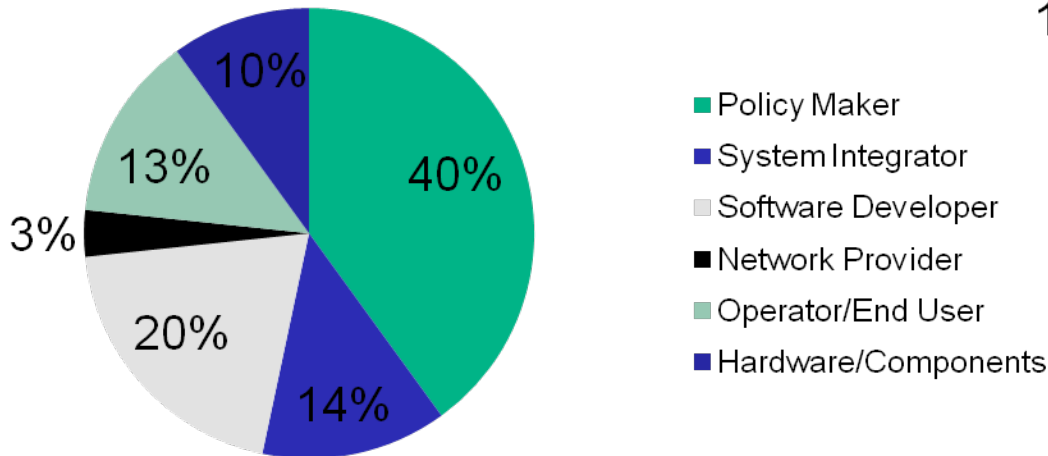
Study Participant Demographics



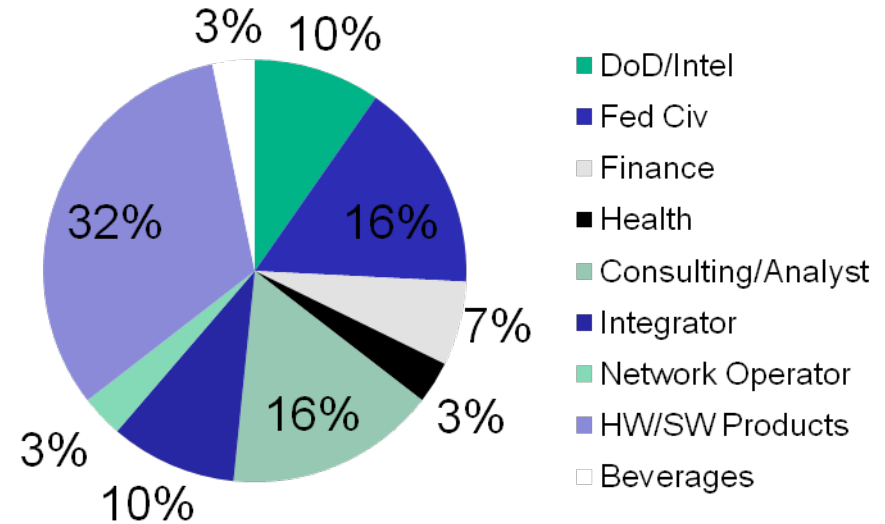
30 Participants Organizations Interviewed



Role



Sector



Use Cases & Abuse Cases



Use Case	Description
Incentives	Develop structured incentives and relationship drivers that facilitate management of shared risk, and facilitate defense-in-breadth across the supply chain
Improve Visibility	Develop technology and best practices to deepen visibility and add coherence and synchronization across the cyber supply chain
Training	Training and education resources for cyber supply chain professionals, investigators, analysts, and auditors

Abuse Cases	Description
Poor Cyber Manufacturing Hygiene	Introduction of malware to consumer electronics through poor supply chain security practices (“apply to” negatively impacting “apply through”)
Supply Chain Denial of Services	Disruption of the supply chain via cyber attack/exploitation
Information Leakage	Industrial espionage that capitalizes on exfiltration of data from supply chain information systems and networks

SDLC/Supply Chain Interdependencies

Synergies within the SDLC & Supply Chain propagate vulnerability compounding impact to the enterprise



Supplier

Your Company

Customer

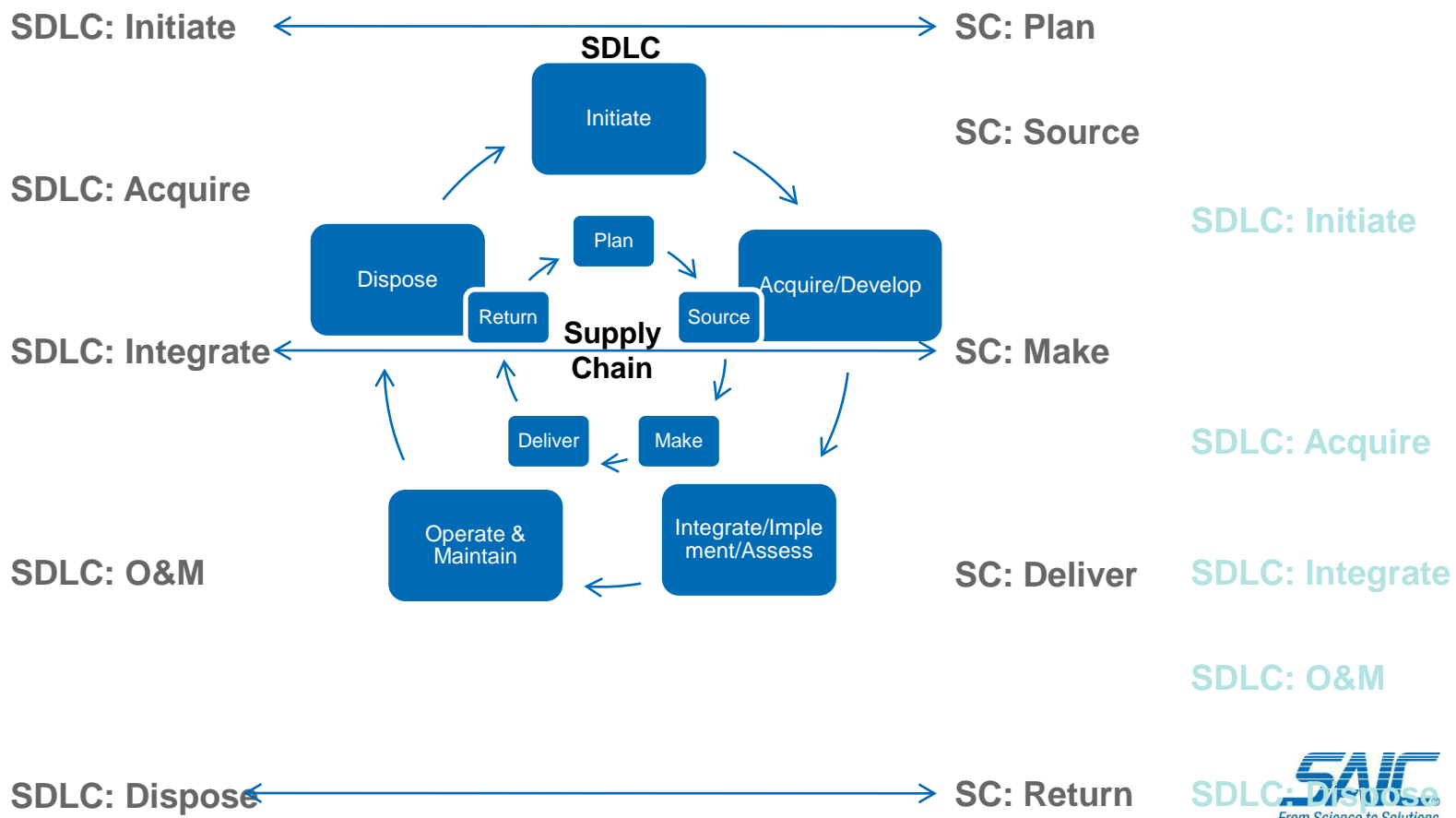
SC: Plan

SC: Source

SC: Make

SC: Deliver

SC: Return

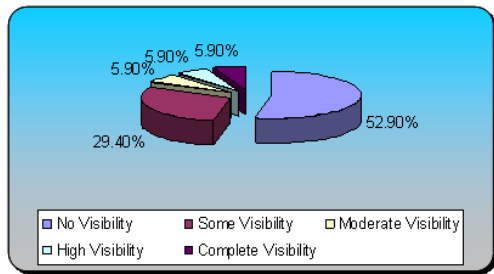


Implementation: Understanding the Use Cases



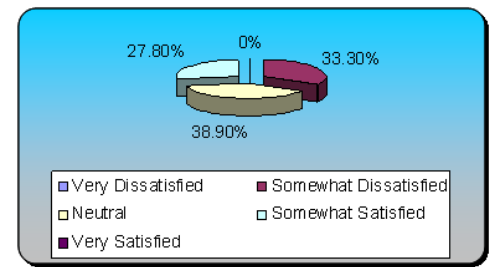
Question 6: How would you rate your visibility into your supply chain partners' operations?

	Responses	
No Visibility	9	52.94%
Some Visibility	5	29.41%
Moderate Visibility	1	5.88%
High Visibility	1	5.88%
Complete Visibility	1	5.88%
Totals	17	100%



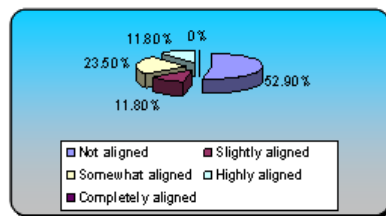
Question 9: To what extent is your information security organization aligned with your supply chain management practice?

Not Aligned	8	47.06%
Slightly Aligned	3	17.65%
Somewhat Aligned	4	23.53%
Highly Aligned	1	5.88%
Completely Aligned	1	5.88%



Question 10: To what extent is your information security operations (SOC/MSS/TOC) aligned with your supply chain risk management center for joint operations?

Not aligned	9	52.94%
Slightly aligned	2	11.76%
Somewhat aligned	4	23.53%
Highly aligned	2	11.76%
Completely aligned	0	0%
Totals	17	100%



Research Conclusions



- A fundamental discovery in this project has been that **global cyber supply chains today are as fragmented and stove piped today as global physical supply chains were a decade and a half ago.**
- There is a **lack of visibility and coherence across the cyber supply chain** which prevents effective orchestration and synchronization.
- A **fully integrated cyber supply chain requires** the coordination of what researchers describe as “**defense in depth**”, the process of securing/hardening core systems and their constituent parts during the build and deploy phases of the lifecycle; and “**defense in breadth**”, the process of securing the global web of actors who use and maintain a system including customers, system integrators and suppliers.
- There is a clear **need for structured incentives** and relationship drivers to facilitate shared management of risk.

Going Forward Together: A Consensual Code Of SCRM Practice



- **Our Cyber Supply Chain Model emphasizes MAD (Mutual Assured Development):**
 - Shared risk identification & accountability through a common Risk Registry.
 - Consensual mitigation practices accomplished by risk “owners” who self-manage the risk.
 - Business objective is to hedge against excessive regulation; to gain greater protection from liability; and to free up financial reserves held for un-insurable risk.
- **Our Model argues for a “Grand Bargain” between Government & Industry:**
 - Streamlined regulations and a simplified set of standards that will lower compliance costs for industry in exchange for formal adoption of a SCRM Code Of Practice by the Key Vendor Community.

Supply Chain Contractual Language



C.3.3 Supply Chain Risk Management (SCRM)

Connections II vendors shall include a Supply Chain Risk Management (SCRM) Plan to address counterfeit and illegally modified products. The SCRM Plan will be reviewed prior to selection.

The Connections II contractor's supply chain consists of organizations, people, activities, information, resources, along with information and communication technology (ICT) equipment, subcomponents and software. The products that are sold, configured, installed and/or maintained under the Connections II contract are provided by Connections II contractors who act as re-sellers of ICT equipment and component OEMs. "Genuine ICT" are ICT equipment, components and software that are authentic - that is, as represented by their suppliers, whether named brand products or commodity products specified only by performance characteristics.

The contractor shall develop, maintain, and periodically update a SCRM Plan, at no cost to the government, to reduce supply chain risks to performance and security of the products sold, installed and maintained throughout the Connections II product/solution life cycle. The Plan shall provide sufficient detail for the government to determine that the contractor reasonably understands its supply chain. The contractor shall ensure that Genuine ICT will be available under the Connections II contract and shall manage the risk to ensure that counterfeit or illegally modified products are not shipped. The Plan shall describe the processes and practices the contractor will employ to ensure that Genuine ICT is delivered to Connections II customers. As a result, a body of evidence shall be generated through SCRM Plan execution. The body of evidence will provide the government assurance that Genuine ICT is available through the contractor's solution.

The SCRM Plan shall address, at a minimum, how the contractor:

1. Ensures within its processes that requirements for Genuine ICT are levied upon its direct suppliers, whether systems integrator, reseller or OEM. The requirements for assurance and supporting evidences shall include:
 1. That the contractor performs reasonable steps to ensure their SCRM Plan will be performed for ICT in its delivered and installed configuration.
 2. That the equipment resellers from whom the contractor purchases ICT have valid licenses for OEM equipment and software.
 3. That the ICT OEM is exercising quality control to ensure that counterfeit or illegally modified hardware or software components are not incorporated into the OEM product.
 4. That the contractor ensures traceability of assurance and evidence of genuineness of ICT back to the licensed product and component OEMs.
2. Ensures that products and components are not repaired and shipped as new products and components provided to the Government.
3. Ensures that supply channels are monitored for counterfeit throughout the product life cycle to include maintenance and repair.
4. Ensures independent verification and validation of assurances and supporting evidence, as required.

Energy | Environment | National Security | Health | Critical Infrastructure





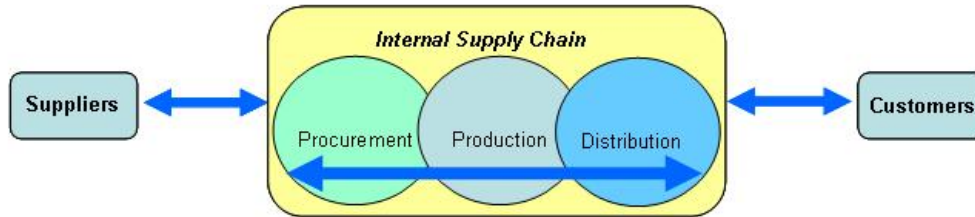
Common Themes for Prevention, Detection and Response

	Physical	Supply Chain	Cyber
Vulnerability Assessments	Assets	HazOp Reviews	IT and Manufacturing & Control Systems, Network
Background Checks	Facility personnel	Vendor credential checks	IT system administrators
Access Control	Facility, restricted areas	Controlled access to Loading areas	Network, sensitive systems
Monitoring	Cameras	Container tracking	Network monitoring software
Awareness	Suspicious activity, thefts	C-TPAT Training	Social engineering, password protection, thefts





FSSCC-FBIIC CYBER SECURITY COMMITTEE SUPPLY CHAIN WORKING GROUP TOOLKIT



Supply Chain Working Group Toolkit:

- [Internal Software Development](#)
- [Services](#)
- [COTS Software](#)
- [Hardware Testing](#)

The FSSCC-FBIIC Cyber Security Committee has sponsored a working group called the Supply Chain Working Group comprised of [leading security and risk management practitioners](#) that have agreed to work together to create a deliverable that will be useful to IT managers and information security officers interested in improving the resiliency of their organization's supply chains.

The Supply Chain Working Group has leveraged resources, practices, information from both the public and private sectors. The intent is to create deliverables that are useful and practical for practitioners that leverage available resources for all industries both private sector and public sector. The members of this working group share a common passion to further the practice and discipline of enterprise wide risk management making it easier of their colleagues to achieve their goals.

The Supply Chain Working Group Toolkit is divided into 4 channels:

1. Internally developed software
2. Software developed by a 3rd-party
3. Software purchased off the shelf
4. Hardware, firmware, appliances

For each channel, the deliverable is divided into 2 sections:

1. A summary of survey results from 4 surveys (1 per channel) of members of FS-ISAC and BITS
2. Identification of leading practices to improve supply chain resilience based on input from recognized subject matter experts including reference information for the growing body of information available on supply chain resilience



SAFECode has released its fourth member report, "**Software Supply Chain Integrity Framework**." The paper outlines the first industry-driven framework for analyzing and describing the efforts of software suppliers to mitigate the potential that software could be intentionally compromised during its sourcing, development or distribution.

[Download Software Supply Chain Integrity Framework Paper \(pdf\) 1.4M](#)



The Software Assurance Forum for Excellence in Code (SAFECode) previously released its member report, "**Fundamental Practices for Secure Software Development**." Based on an analysis of the individual software assurance efforts of SAFECode members, the paper outlines a core set of secure development practices that can be applied across diverse development environments to improve software security.

[Download Development Practices Paper \(pdf\) 2.1M](#)

Source: <http://www.safecode.org/>



Identification of High Priority Systems

SCRM Thresholds	DCID		DOD		NIST/CNSS ^[1]
	Availability/ Integrity Level of Concern (LOC)	Minimum Protection Level (PL)	Minimum Mission Assurance Category (MAC) Level ^[2]	Minimum Confidentiality Level ^[3]	Availability/Integrity/Confidentiality Impact Level
High Assurance	High	PL1	MAC 1	Sensitive	High
Medium Assurance	Medium	PL1	MAC 2	Sensitive	Moderate
Low Assurance	Basic	PL1	MAC 3	Public	Low

- [1] CNSSI 1199 is in draft format and addresses the security categorization for NSS.
- [2] Mission assurance categories are primarily used to determine the requirements for availability and integrity.
- [3] The SCRM Threshold for High Assurance includes the confidentiality level of classified for all MAC levels.



Lifecycle Risk Mitigation Approach

Life Cycle Stages	Design	Manufacturing	Integration	Distribution	Operations	Services/ Maintenance	Retirement
Sample Protective Measures	- Use vetted providers and industry best practices	- Employ service level agreements related to quality and security	- Limit online SW installations - Thoroughly vet updates	- Use secure distribution channels	- Implement and enforce traditional information assurance policies	- Confirm the integrity of network mapping	- Secure destruction of media and computers

To meet tomorrow's threat we must develop protection measures across product lifecycle *and* reinforce these measures through acquisition processes and effective implementation of agency security practices



Source: NIST ISPAB, April 2009



DHS 24 Core “Concern Categories”:

- - Organizational History
- - Foreign Interests and Influences
- - Security "Track Record"
- - Financial History and Status
- - Individual Malicious Behavior
- - Software Security Training and Awareness
- - Software History and Licensing
- - Development Process Management
- - Software Development Facility
- - Concept and Planning
- - Design
- **Software Development**
- **Component Assembly**
- **Testing (supply-side)**
- **Installation and Acceptance**
- **Software Change Management**
- **Built-in Software Defenses**
- **Assurance Claims and Evidence**
- **Software Manufacture and Packaging**
- **Support**

Source: Dept. Homeland Security, Software Assurance in Acquisition: Mitigating Risks to the Enterprise

A Reference Guide for Security-Enhanced Software Acquisition and Procurement
National Security | Health | Education | Environment
October 22, 2008



Collaborative Security Models



Collaborative security models are security solutions that are:

- Ecosystem-driven
- Eventually consistent
- Real time
- Fully integrate human intelligence tasks through an architecture of participation



In the past, you would make a decision.

In the future, you will rewrite the algorithm.

Questions?



Energy | Environment | National Security | Health | Critical Infrastructure



Trademark Attributions



Flickr is a registered trademark of Yahoo Inc. in the U.S. and/or other countries.

Facebook is a registered trademark of Facebook, Inc. in the U.S. and/or other countries.

BlogPulse is a registered trademark of Buzzmetrics Ltd. in the U.S. and/or other countries.

Twitter is a registered trademark of Twitter, Inc. in the U.S. and/or other countries.

Symantec is a registered trademark of Symantec Corporation in the U.S. and/or other countries.

YouTube is a registered trademark of Google Inc. in the U.S. and/or other countries.

Hulu is a trademark of Hulu, LLC in the U.S. and/or other countries.