UNIVERSITY OF MARYLAND

ROBERT H. SMITH SCHOOL OF BUSINESS

Developing A Cyber Supply Chain Assurance Reference Model

A Research Collaboration Between SAIC
& The R.H. Smith School of Business University Of Maryland
Presenters: Dr. Sandor Boyson & Mr. Hart Rossman

April 2, 2009

SAIC
From Science to Solutions

Project Overview

- 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 Supply Chain Management Center of the Robert H. Smith School of Business, University of Maryland College Park is undertaking collaborative research with SAIC to develop a supply chain assurance reference model for cyber infrastructure.

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

SAIC
From Science to Solutions

Project Milestones

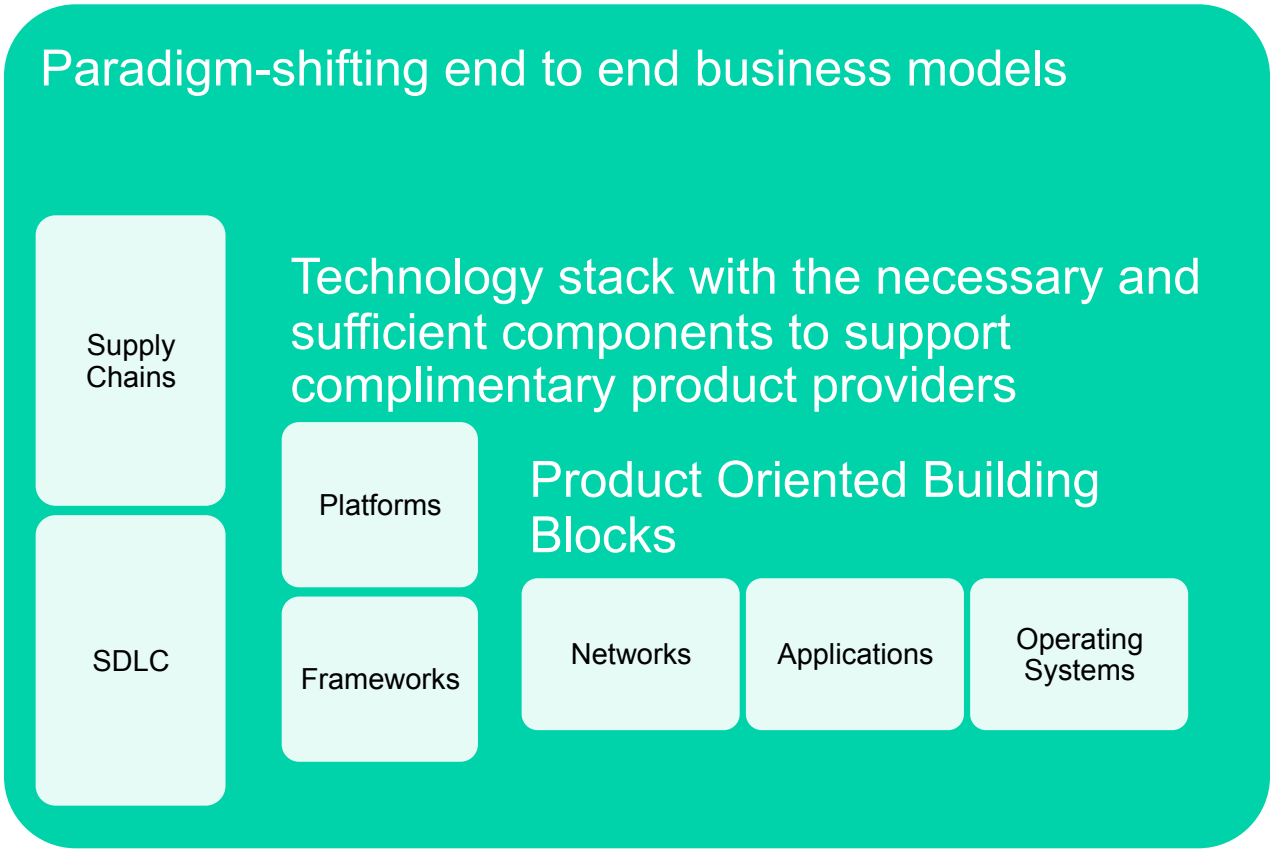
- Phase 1: Literature Review and Interview Guide Development (October –November 08).
- Phase 2: Conduct interviews with 25-30 thought leaders in the systems engineering, network management , software/ hardware development, human factors and supply chain risk management areas (November 2008–February, 2009).
- Phase 3: Compile interview results, analyze findings, and prepare a Prototype Cyber- Supply Chain Assurance Reference Model for presentation to a focus group convened by SAIC of 30-45 government and industry executives (March, 2009).
- Phase 4: Results of this feedback will be incorporated into a final research report (April, 2009).

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

SAIC
From Science to Solutions

Project Rationale:

The current threat landscape requires a convergence between "Defense In Depth" & "Defense In Breadth".



In the digital age, sovereignty is demarcated not by territorial frontiers but by supply chains. – Dan Geer, CISO In-Q-Tel

Amateurs study cryptography; professionals study economics. -Allan Schiffman

Project Rationale (1):

The current threat landscape requires a convergence between "Defense In Depth" & "Defense In Breadth".

Synthesis

Analysis

- Supply Chains
- SDLC
- Platforms
- Frameworks
- Applications
- Networks
- Operating Systems

Risk Management

Compliance

Project Rationale (2) :

The current threat landscape requires a convergence between "Defense In Depth" & "Defense In Breadth".

Integration of People, Process, and Technology

Technology & Product Focus

- Supply Chains
- SDLC
- Platforms
- Frameworks
- Applications
- Networks
- Operating Systems

Risk Management

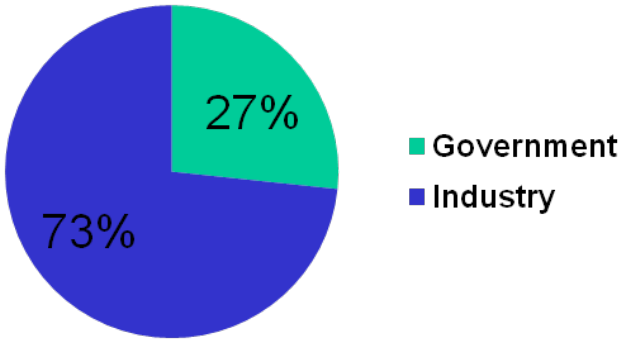
Compliance

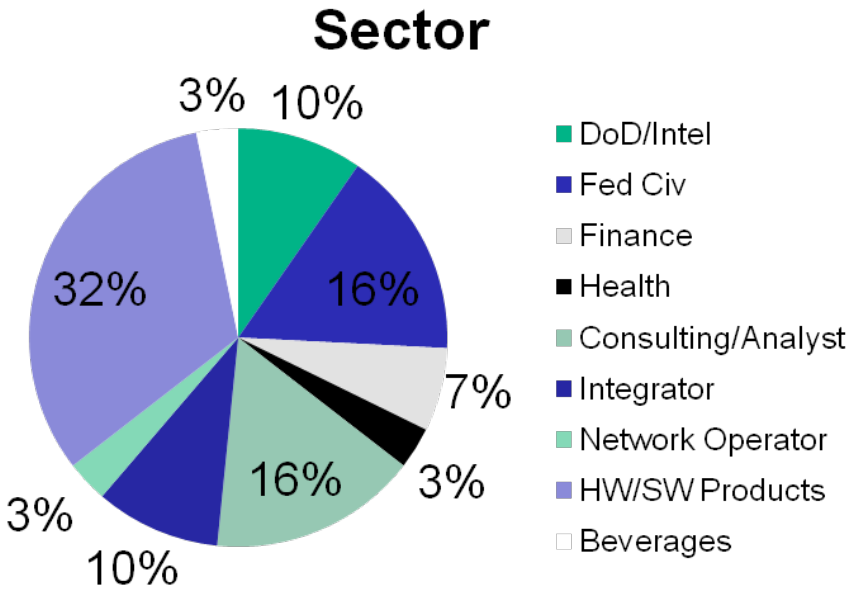
UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

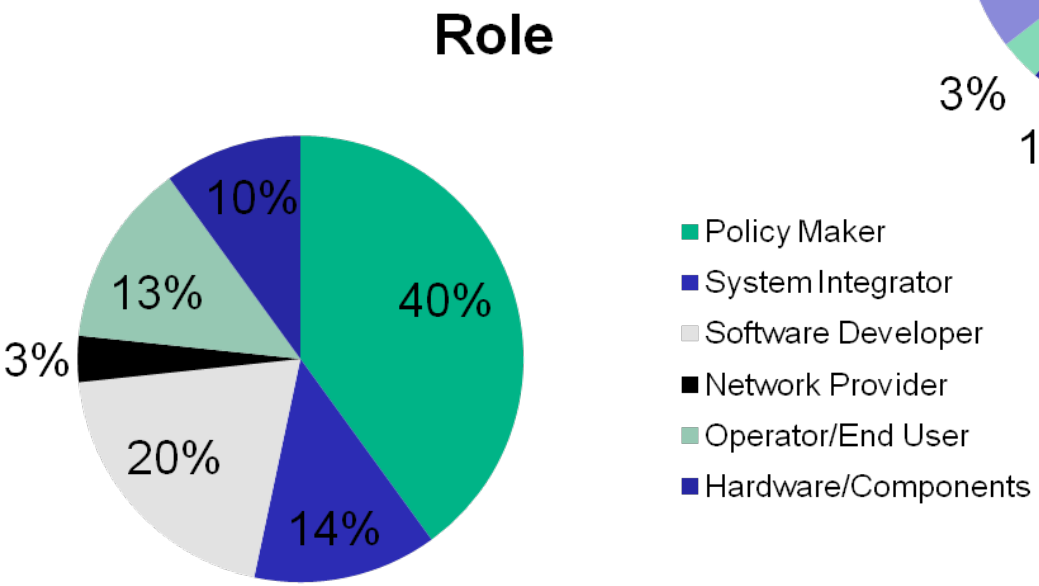
SAIC
From Science to Solutions

Study Participant Demographics

30 Participants Interviewed







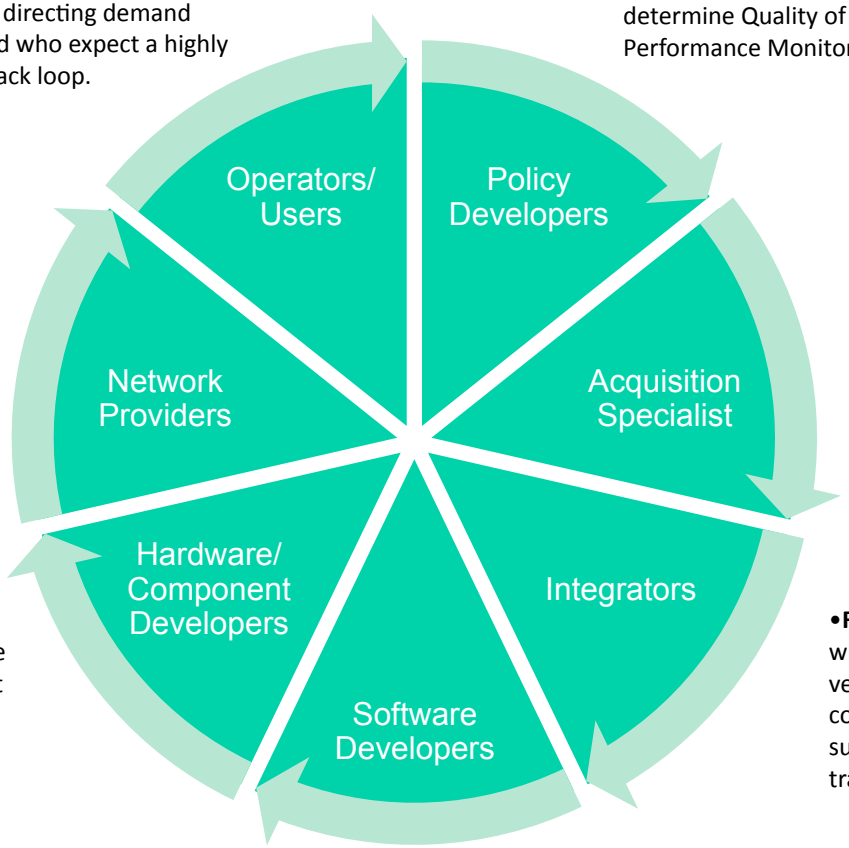
UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

SAIC
From Science to Solutions

Cyber Supply Chain Actors

•**Responsibilities**:
must maintain the highest trust levels in the system, who must have clear paths for directing demand signals to the supplier base and who expect a highly responsive supply chain feedback loop.

•**Responsibilities**:
prepare concepts of operation (Con Ops) and who determine Quality of Service (QOS) and Supplier Performance Monitoring Standards.



•**Responsibilities**:
must manage Tier II suppliers, assure production quality and guard against counterfeits entering the system.

•**Responsibilities**:
seek to embed federal acquisition regulation (FAR) changes into procurement contracting in pursuit of greater supply chain assurance.

•**Responsibilities**:
must manage Tier II suppliers, assure production quality and guard against counterfeits entering the system.

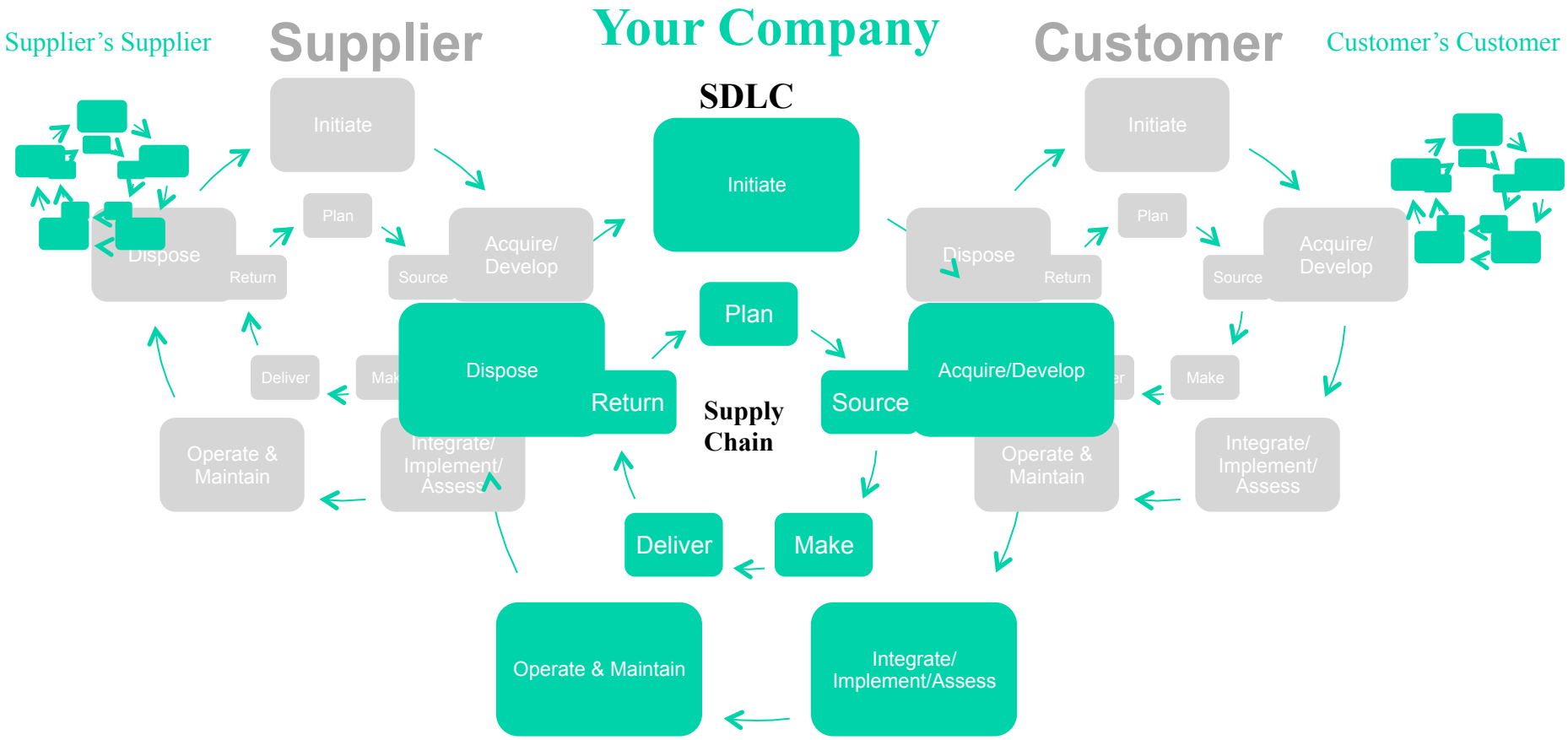
•**Responsibilities**:
who act as Tier I coordinators of cross-vendor products and services and who seek common criteria for evaluation of Tier II suppliers and more secure cross-vendor transaction/communication platforms.

•**Responsibilities**:
manage software pedigree, code integrity, and kernel evaluation assurance levels and try to carefully screen human or viral threats to their processes.

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

SAIC
From Science to Solutions

SDLC/Supply Chain Ecosystem



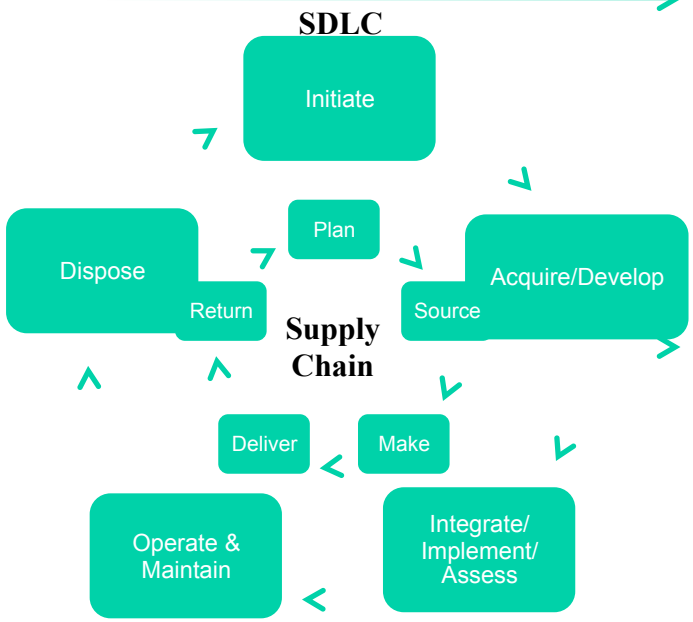
SDLC/Supply Chain Interdependencies

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

Supplier | **Your Company** | **Customer**

SC: Source

SDLC: Initiate ⟷ SC: Plan



SC: Make

SC: Source

SDLC: Acquire

SDLC: Initiate

SC: Deliver

SDLC: Integrate

SC: Make

SDLC: Acquire

SDLC: O&M

SC: Deliver

SDLC: Integrate

SDLC: O&M

SC: Return

SDLC: Dispose

SC: Return

SDLC: Dispose

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

SAIC
From Science to Solutions

Early Research Insights

- A fundamental discovery in this project was 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.
  - The RH Smith Supply Chain Management Center studied hundreds of companies in the early 1990s that were undertaking global supply chain transformation and see a profound similarity between the struggles of cyber-supply chain managers today and the struggles of those earlier supply chain managers to gain visibility over operations and to establish more collaborative & robust business ecosystems with customers, distributors and suppliers on a worldwide basis.
  - Supply chain managers needed to create a process map and set of activity definitions to capture the operational complexity they faced and begin to create effective management understandings and responses. A consensus emerged around the Supply Chain Operations Reference (SCOR) Model developed by the Supply Chain Council, a membership group of over 800 companies, which now is the widely accepted industry standard.
- Lack of visibility and coherence across the cyber supply chain
- Need for structured incentives and relationship drivers which facilitate management of shared risk
- Lack of communication between the cyber and physical supply chain domains is constraining advancement
- The concept of “apply to” and “apply through” is key to understanding the interdependencies between SDLCs across the supply chain which drive the need for an evolutionary approach to shared risk management.

Contact Info

Sandor Boyson

Co-director, Supply Chain Management Center

Research professor logistics and public policy dept.

Robert H. Smith School of Business
3355 Van Munching Hall
University of Maryland
College Park, MD 20742-1815

301-405-2205

sboyson@rhsmith.umd.edu

Hart Rossman

Vice President, CTO Cyber Programs
SAIC

Senior Research Fellow, Robert H. Smith School of Business

SAIC

1710 SAIC Drive

M/S T3-6-5

McLean, VA 22102

703-676-5598

rossmanh@saic.com

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

SAIC
From Science to Solutions