RSA Conference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: STR-F03

Supply Chain as an Attack Chain:
Key Lessons to Secure Your Business

MODERATOR:

Tony Gaidhane
Senior Associate
Booz | Allen | Hamilton
@Tony_Gaidhane

PANELISTS:

Scott Stephens
Director, EG Global Supply Chain
HP

Sam Phillips
VP, GM, CISO
Samsung Business Services
@Sam_Phillips_se

Benjamin Jun
CTO
Chosen Plaintext
@BenjaminJun

Agenda

- **Motivations and Drivers**
  - Adversarial Supply Chain Operations (ASCO)
  - Maturing Customer Requirements (Public vs. Private Sector) and Regulations
  - Threat Actors
- **Capabilities of a mature Supply Chain Cyber Risk Management (SCCRM) Program**
  - Tools and Techniques
    - Counterfeit Resistant Chips (crypto key pairs)
    - Security by Design
  - Visibility and Traceability
    - Component Tracking
  - Cyber Security Testing and Options
  - Product Security Incident Response
  - The future of SCCRM
- **Wrap-up and Q&A**

Adversarial Supply Chain Operations (ASCO) To vs. ASCO Through

Adversaries

- Nation State Actors
- Competitors (esp. Nation State-owned)
- Criminals
- Hacktivists

Lifecycle Process

Design | Sourcing | Build | Fulfillment | Distribution | Sustainment & Operations | Disposal

ASCO *To*

Methods:
- Interdiction/ Compromise
- Theft/ Re-Route
- Break/Fix Subversion

Effects:
- Halt or slow production
- Prevent sustainment operations
- Loss of Intellectual Property

ASCO *Through*

Customer Operations

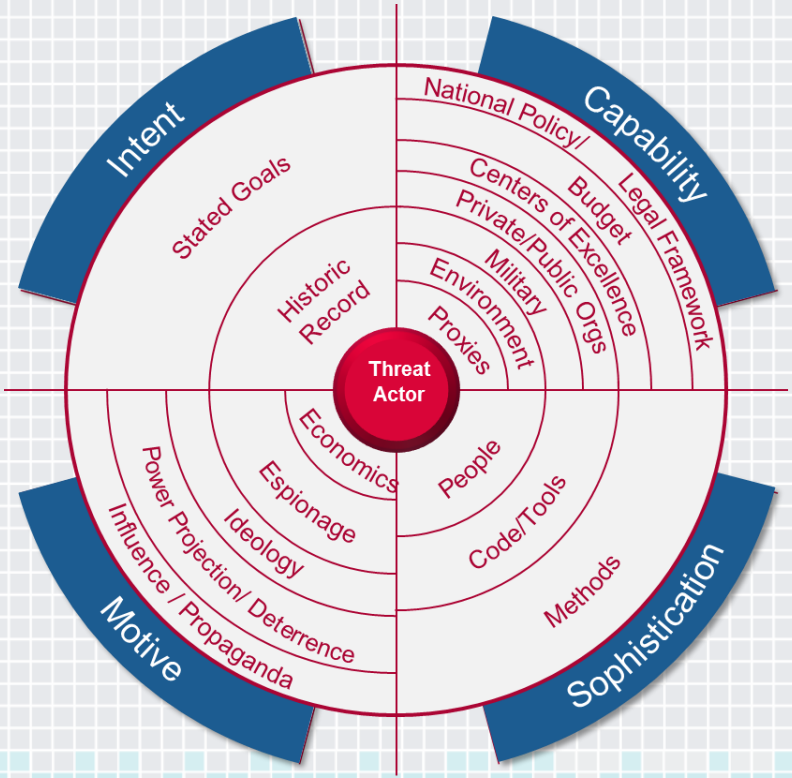
Methods:
- Malware Shotgun Infection
- Malicious Component Insertion
- Repair part compromise
- Trojan Insertion/Design to Fail

Effects:
- National security risk
- Customer compromise
- Impaired customer operations
- Brand/ Legal/ Market Impact
- Loss of customer intellectual property

Public Sector Requirements

- **Cyber Hygiene Practices of Third Parties**
  - Executive Order 13636 PD 21
  - NIST Cyber Risk Management Framework
  - Voluntary Implementation for Critical Infrastructure
- **Product Integrity/ Software Assurance And Hardware Assurance (Anti-Counterfeit)**
  - GSA/DOD Improving Cybersecurity Through Acquisition Recommendation V
  - Using Commercially Acceptable Global Sourcing Standards And Evaluation Of Context And Fit For Use
- **Malicious Insertion During Development**
  - DODI 5200.44 - Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)
  - NIST SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations

Understand your adversary



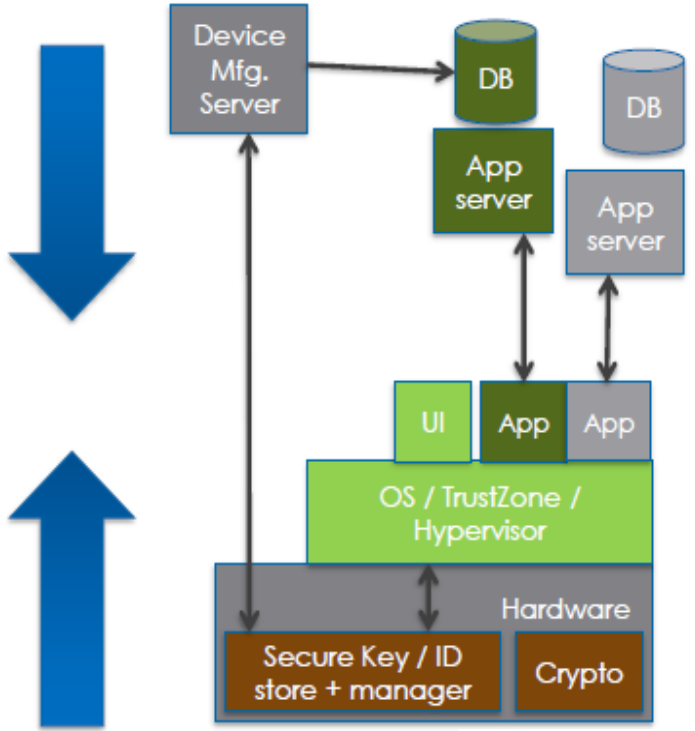
Agenda

- **Motivations and Drivers**
  - Adversarial Supply Chain Operations (ASCO)
  - Maturing Customer Requirements (Public vs. Private Sector) and Regulations
  - Threat Actors
- **Capabilities of a mature Supply Chain Cyber Risk Management (SCCRM) Program**
  - Tools and Techniques
    - Counterfeit Resistant Chips (crypto key pairs)
    - Security by Design
  - Visibility and Traceability
    - Component Tracking
  - Cyber Security Testing and Options
  - Product Security Incident Response
  - The future of SCCRM
- **Wrap-up and Q&A**

Trust meets in the Middle

Identity + key provisioning
Authentication service
Secure session management
Security updates

Identity + key management
Sandboxed secrets
Partitioning of critical state
Reliability & integrity



Source: https://www.src.org/calendar/e005440/starss-benjaminjuni-secure-systems.pdf

Characterize Your Threats

Benefit / Payoff Factors

Risk Factors

Cost / Resource Factors

Threat Payoff

Value placed on the rewards

Adversary Confidence

Assessed likelihood the supply chain attack accomplishes its goal

Risk of Detection

Likelihood of detection

Risk of Attribution

Likelihood of suspect being identified

Scope of Retribution

Likely accessed scope of client's response

Tools

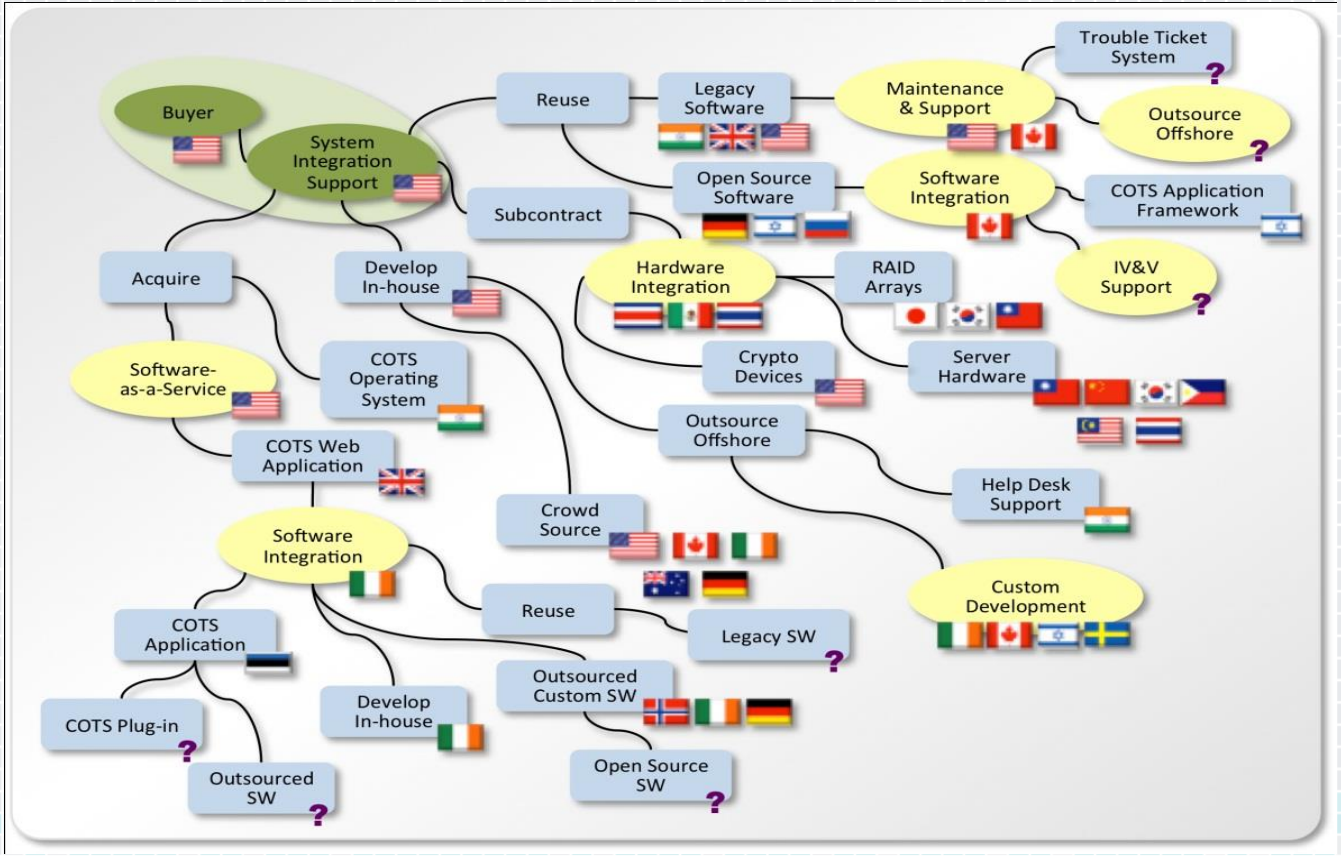
sophistication of the cyber and other tools being used

Techniques

Sophistication of the tactics, techniques, and procedures

Characterization Factors

Test This?


Buyer
System Integration Support
Reuse
Legacy Software
Maintenance & Support
Trouble Ticket System
Outsource Offshore
Subcontract
Open Source Software
Software Integration
COTS Application Framework
Acquire
Develop In-house
Hardware Integration
RAID Arrays
IV&V Support
Software-as-a-Service
COTS Operating System
Crypto Devices
Server Hardware
COTS Web Application
Outsource Offshore
Help Desk Support
Crowd Source
Software Integration
Custom Development
Reuse
Legacy SW
COTS Application
Outsourced Custom SW
Develop In-house
COTS Plug-in
Open Source SW
Outsourced SW

Apply What You Have Learned Today

- Next week you should:
  - Conduct a Supply Chain Decomposition and Identify High-Priority Components
- In the first three months following this presentation you should:
  - Conduct a Threat Assessment (Outside-in, Open Source, Threat Vectors)
  - Characterize your Risks (Business Impact Analysis, Inherent Risks)
  - Understand your Baseline Capabilities (including Compliance Posture)
- Within six months you should:
  - Conduct a Gap Analysis, and define Target State Maturity
  - Identify Key Priorities for Visibility, Control and Governance

Comprehensive SCCRM Program Maturity

Control Implementation of technical capabilities	• Supplier Assessments • Supplier Contractual Amendments • R&D Engagement across Supply Chain • Collaboration with Threat Intelligence	• Segmentation of Proprietary Data • Automatic Security Checks • Standardized Software Security Testing • High Assurance Product Maturity Model
Governance Oversight, monitoring, and collaboration with supplier cyber operations	• Database of Cybersecurity Requirements • Organizational Structure & Design • Cybersecurity Engagement Tool • Strategy Development	• Legal Requirements for Suppliers • Formalized Cyber Organizational Functions • Procedures for Vulnerability ID • Risk Management Framework & Function
Ongoing Visibility Comprehensive, timely, and dynamic vision over key cyber components	• Supply Chain Cybersecurity Assessment • Component Sourcing • Integration of Incident Response • Repair/Replace Parts Management • Counterfeiting Detection	• Consolidation of BOM Tools • Cybersecurity Performance Management • Monitoring of Emerging Risks • Awareness of Cybersecurity

RSAConference2015

San Francisco | April 20-24 | Moscone Center

QUESTIONS?