Information Sharing: The Past, Present and Our Future

Chandra McMahon
Lockheed Martin
Chief Information Security Officer

LOCKHEED MARTIN

Threat Information Sharing Journey

- The Road We’ve Travelled
- Current Landscape
- Navigating for Tomorrow

Why Share Information?

- Drive Intelligence-Driven Defense
- Beyond Indicators & Warnings
- Community Collaboration Expands Feedback Loop
- Builds Trusted Community Partnerships
- Maximizes Public and Private Sector Partnerships

Sharing Leads to Increased National Security

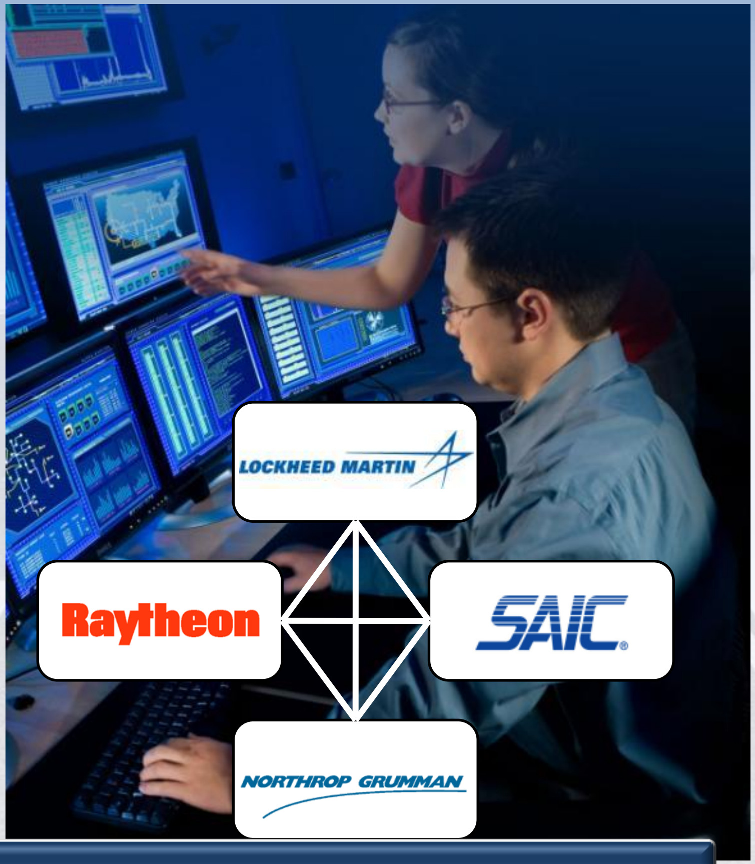
Looking Back (Prior to 2005)

- Broad-based threats were dominant issue
- Government recognition of advanced threat
- Compliance was the measure for security
- Companies have small (if any) CIRT
- Security analysis "outsourced" to AV and IDS vendors

"My antivirus and COTS IDS signature will protect me."

The Awakening (2005 – 2006)

- **Sophisticated, targeted intrusions impact Public & Private sector**
- **Corporate internal investments ramp up**
- **Information sharing formalizes**
  - Special Access NDAs between industry and LE/CI
  - Air Force partners with industry
  - DoD program specific agreements
  - NDAs develop between several major defense companies



Creating Value through Public & Private Partnerships

Formalization (2007 – 2009)

- **2007– Single, scalable DoD-defense industry partnership takes shape**
  - DEPSECDEF England and DIRNSA brief CEOs of 11 key defense contractors at the Pentagon
  - DIB Cyber Task Force and Defense Collaborative Information Sharing Environment (DCISE)
  - Enables classified-level threat Intel sharing (DIBNET)

- **2008 – Industry-led DSIE for rapid information sharing**
  - Mutual NDA and secure portal enables analyst-to-analyst info sharing, collaboration
  - Quickly has 30+ DIB companies sharing real-time

Success Stories

- Creating real-time situational awareness
- Industry members mature from consumers to producers
- Government and Industry collaboration

Stronger Together through Information Sharing

Public Awareness

- 2005 – Time Magazine, Washington Post first detail APT activity
- 2009 – Google Aurora incident
- 2010 – STUXNET and Details of Buckshot Yankee Release
- 2011 – Numerous incidents reported

Where are we today?

- **Consolidating overlapping information sharing groups**
  - Industry groups integrating (DSIE, NSIE, ADMIE)
  - Government efforts consolidating (CYBERCOM, NCCIC)
  - Public/Private “Kill Chain” analysis workshops
  - Collaboration is faster & broader than ever before
- **Challenges remain**
  - Significant gaps in linking public/private partnerships
  - Multiple government entities establishing “cyber” responsibilities
  - APT focus shifting to supply chain (small to mid sized companies)
  - Cross-sector collaboration

What does the Future bring?

- Legislative/Regulatory Requirements

- Agile Response to Ever Changing Threat Landscape

- Information Sharing Ecosystem

Legislative/Regulatory Changes

- **Numerous cyber bills introduced by Congress**
- **Administration weighing in**
- **New DFAR Regulations**
- **Contract clauses to protect unclassified DoD data**

CYBERSPACE POLICY REVIEW

Assuring a Trusted and Resilient Information and Communications Infrastructure

Risk of Being Overburdened by Paper Security

Agile Response to Changing Threats

- Moving from information sharing to active blocking
- Security vendors facilitating more intelligence-driven response in tool set
- Targeting of mobile assets
- Adversary Moving from Exploitation to Attacks

Growing Supply Chain Risk

- Attacker shifting focus to smaller companies
- Data stolen from supply chain puts technology at risk
- CNA against supplier disrupts operational capabilities
- Data integrity harder to assure
- Delivery of counterfeit components

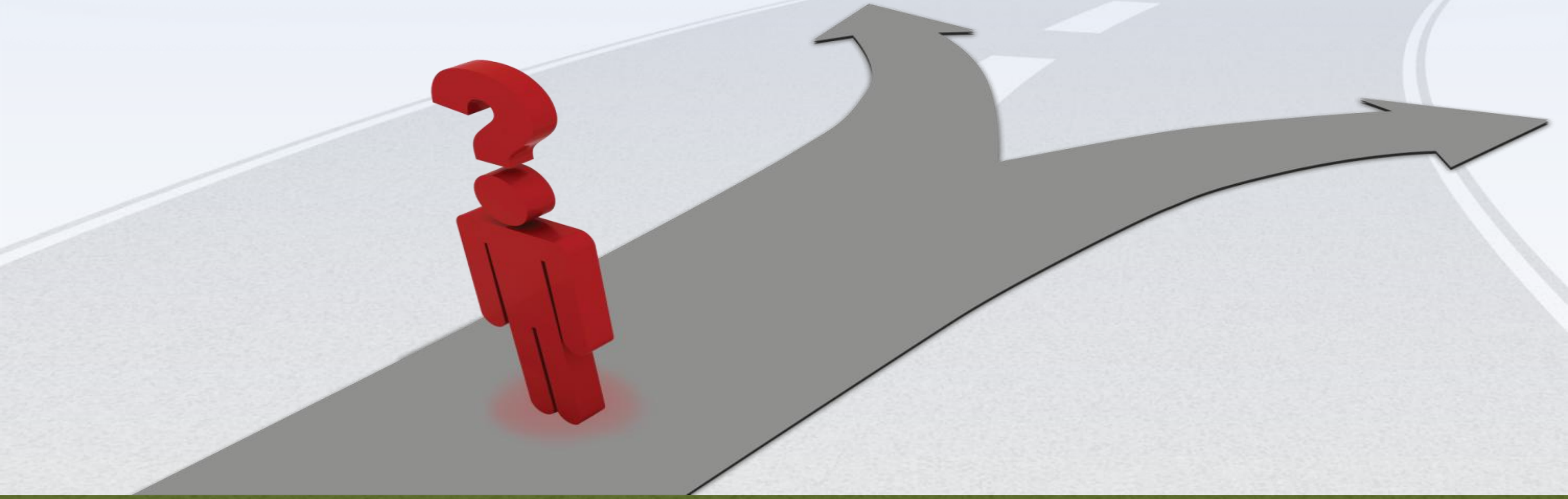
Engaging Supply Chain in Information Sharing Vital to Success

The New Information Sharing Ecosystem

- **Design & Operationalize New Model**
  - – Eliminate current challenges
  - – Agile & affordable
  - – Tiered system
  - – Engage broader community

Information Sharing Challenges

- **Avoiding the pitfalls of counterproductive collaboration**
  - Increased OPSEC risks
  - Information dilution, misjudging significance
  - Intelligence echo and negative feedback loop



Shift Threat Sharing Direction

- **Focus on Trusted Information-Sharing "Bridges"**
  - True partnership
  - Government and industry working together
  - Near real-time
  - Formatted data structures
  - Fewer information silos

Enhance Information Sharing Infrastructure to Ensure Future Success

Trusted Bridge Benefits & Approach

- **Benefits**
  - Common understanding of threats & priorities
  - Greater transparency between public & private sectors
  - Greater international information exchange

- **Approach**
  - Smaller companies will need MSSP
  - Data interchange formats enable faster processing
  - Pay-to-play model supports necessary infrastructure

A New Ecosystem

- Continuing Threats
- Richer Partnerships
- Greater Information Sharing