Quantifying Defense Supply Chain Economic Impact: Strategies For Creating Value Amid Volatility

Panel Discussion

Protecting the Digital Thread

Global Supply Chain Summit
June 26, 2014

Michael McGrath, ANSER
michael.mcgrath@anser.org
Protecting the Digital Thread

Panelists

**Michael McGrath**, Vice President, Systems and Operations Analysis, Analytic Services Inc.

**Dan DiMase**, Director, Compliance and Quality, Honeywell International Inc.

**John Toomer**, Director, Intelligence, Information & Cyber Systems, Government Operations, The Boeing Company
Advanced Manufacturing is:

- Driven by a “Digital Thread” of product and process information – valuable intellectual property (IP)
- Networked at every level to gain efficiency, speed and quality
- Targeted by global cyber threats

Common Visions
Smart Manufacturing,
Industrial Internet,
Industry 4.0, …

The Internet of Things!

Manufacturing is a Cyber-physical Business
The Threat is Global and Growing

Manufacturing is an inviting target

IBM Security Services Cyber Security Intelligence Index 2014

Manufacturing: a 1 in 3 chance of being targeted by at least one Spear Phishing attack in 2013

Symantec Internet Security Report 2014

Cost to Global Economy > $400 B

IBM Security Services Cyber Security Intelligence Index 2014

WHO’S SPYING ON YOU?

No business is safe from cyber-espionage
NDIA White Paper
Protecting the Digital Thread

Manufacturing Concerns:

• Theft of technical info -- can compromise national defense and economic security

• Alteration of technical data -- can alter the part or the process, with physical consequences to mission and safety

• Disruption or denial of process control -- can shut down production

A risk management problem. Need resilience!
Scope: Protecting the Digital Thread
Technical Data in the Advanced Manufacturing Enterprise

Targeted by nation states, terrorists, criminals and hacktivists.

Digital Interchange and Online Access

Customer Data Systems

Enterprise IT System

Product Support System

Engineering Data System

Product & Process Data

Manufacturing Operations Systems

IT Cyber Security Solutions May Not Fit Manufacturing Operations Needs
What We Heard from Interviews

Gov’t, Industry, Academia

- CIOs/CISOs in the defense primes are implementing strong cyber risk management and sharing info through the DIB CS/IA and DSIE programs
  - Concerned about suppliers and willing to work with them
  - Have not yet seen threat to factory systems, but acknowledge the possibility
  - Need cost/risk tradeoffs to arrive at an affordable solution

- Industrial Control Systems (ICS) are soft targets. Culture differs from IT.
  - Standards and guides* for ICS provide good risk management approaches. Implementation is spotty.

- DoD has mandated protection of critical information
  - Primes address in the program protection plan, but ICS security is not emphasized in DoD guidance

- Defense R&D for cybersecurity is not currently focused on factory floor

*E.g. ANSI/ISA99 standards and NIST SP 800-82
Operational Technology (OT) vs. IT

What’s Different?

- ICS systems are long-lived capital investments (15-30 year life)
  - Old processors, operating systems, protocols, and configuration control.
  - New systems architected for security, but hard to integrate with old

- “Production mindset” with little tolerance for OT down time
  - Operate in real time with critical safety implications – cannot install patches without scheduled downtime and testing
  - System availability valued over integrity or confidentiality. Weak privilege management among operators and maintainers who troubleshoot the systems. Growing use of wireless devices.
  - Nascent cybersecurity awareness. Poor password management, etc.

- Manufacturing differs from other ICS applications (Power Grid et al.)
  - Every manufacturing job brings new executable code into system
  - Tech data flowing through the system is a target
Recent Developments

- **Federal Register 18 Nov 2013 -- DFAR 252.204–7012 Safeguarding of unclassified controlled technical information.**
  - Specifies 54 minimum security controls linked to NIST SP 800-53
  - Reporting of cyber incidents to DoD within 72 hours
  - Reviews and data retention to support DoD Damage Assessments
  - Mandatory flow-down to subcontracts

- **NIST Cybersecurity Framework for Critical Infrastructure Protection (Feb 2014)**
  - Common vocabulary, core standards and practices
  - Risk-based. Voluntary adoption.
  - Sector-specific implementation, including training and incentives.
NDIA White Paper
Recommendations for USD(AT&L)

1. Designate a focal point to work with industry on risk-based, voluntary standards and practices for factory floor cybersecurity.
   - Evaluate NIST framework as starting point.

2. Conduct forums with industry to help understand and implement DFARS clause, including factory floor implications.

3. Update DoD guidance on the Program Protection Plan (PPP). Let industry make appropriate risk/cost tradeoffs.

4. Use red teams to expose vulnerabilities and R&D to fill gaps

5. Assist SME suppliers with training and investments
   - NIST Manufacturing Extension Partnership to deliver training
   - Defense Prod Act Title III and Manufacturing Technology investments
   - Training for DoD contracting officers
Protecting the Digital Thread

Panelists

Michael McGrath, Vice President, Systems and Operations Analysis, Analytic Services Inc.

Dan DiMase, Director, Compliance and Quality, Honeywell International Inc.

John Toomer, Director, Intelligence, Information & Cyber Systems, Government Operations, The Boeing Company