Managing Risk in the Supply Chain

Moderator:
Derek Harp, ICS Security, SANS Institute

Panelists:
Nadya Bartol, VP Industry Affaires and Cybersecurity Strategist – UTC
Samara Moore, Senior Manager CIP Security and Compliance – Exelon
Melanie Seader, Senior Cyber and Infrastructure Security Analyst – EEI
Doug Wylie, Director – Industrial Security Program, Rockwell Automation
Supply Chain Risks Affect ICS Security

“Incapacity or destruction” may have a “debilitating impact on security, national economic security, national public health or safety...”

Added Potential Impacts

- Personal safety (employees and operators)
- Loss or damage to physical assets
- Regulatory fines for non-compliance
- Disturbances to manufacturing schedules
- Theft of intellectual property and know-how
- Reputational damage (brand image)
# Managing Supply Chain Cyber Security Risks

<table>
<thead>
<tr>
<th>Process</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Risk based approach</td>
<td>- Understand connectivity</td>
</tr>
<tr>
<td>- Enterprise policy</td>
<td>- Architecture, design to reduce risk</td>
</tr>
<tr>
<td>- Establish security requirements</td>
<td>- Monitor changes and anomalous activity</td>
</tr>
<tr>
<td>- Incorporating terms and conditions into contracts</td>
<td></td>
</tr>
<tr>
<td>- Consistent evaluation of security req</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>People</th>
<th>Available Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Involves all stakeholders: IT, Security, Legal, Procurement, Business Units</td>
<td>- DHS Cyber Security Procurement Language for Control Systems</td>
</tr>
<tr>
<td>- Training</td>
<td>- Cybersecurity Procurement Language for Energy Delivery Systems</td>
</tr>
<tr>
<td>- Ensure following policy and process</td>
<td>- EPRI Cybersecurity Procurement Requirements Traceability</td>
</tr>
<tr>
<td>- Follow through with ensuring supply chain requirements are met and periodic evaluations</td>
<td></td>
</tr>
</tbody>
</table>
Process Example: Consistent Evaluation of Requirements

Internal Purchasing Questionnaire

Prior to supplier selection, assess:
• Criticality of the purchase to the organization;
• Potential for business or service disruption;
• Potential for data loss;
• Potential value of the new purchase to the business;
• Connectivity to other critical systems.

Vendor Security Questionnaire

Use available guidance to assess security capabilities:
• Provide a qualitative questionnaire leveraging categories in the NIST Cybersecurity Framework;
• Use the DOE industry guidance to map to ES-C2M2, as a qualitative assessment;
Include relevant internal security standards in the vendor questionnaire.
Technology Example: Security Architecture

Architecture

- Understand the systems and data flows
- Is remote access required
- Can system be designed to minimize risk
- Can system be monitored to identify changes or activity outside of the baseline

Security Requirements

- Practices followed on your network should apply to any systems that may access your network, or which your network may access
- Include provisions in contract language to allow for auditing or verification of security practices
Managing Cyber Supply Chain Risk

- Cyber supply chain risk management is a shared responsibility
- Managing cyber supply chain risk requires cross-functional coordination
- Managing cyber supply chain risk is a continuous process
- Information and communication technology (ICT) must be built using secure development practices
- Cybersecurity must be built into ICT systems
- Cybersecurity must be verified throughout the lifecycle of ICT
## Dell Inspiron 600m Notebook: Key Components and Suppliers

<table>
<thead>
<tr>
<th>Component</th>
<th>Supplier or Potential Suppliers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel Microprocessor</td>
<td>US-owned factory in the Philippines, Costa Rica, Malaysia, or China (Intel)</td>
</tr>
<tr>
<td>Memory</td>
<td>South Korea (Samsung), Taiwan (Nanya), Germany (Infineon), or Japan (Elpida)</td>
</tr>
<tr>
<td>Graphics Card</td>
<td>China (Foxconn), or Taiwanese-owned factory in China (MSI)</td>
</tr>
<tr>
<td>Cooling fan</td>
<td>Taiwan (CCI and Auras)</td>
</tr>
<tr>
<td>Motherboard</td>
<td>Taiwan (Compaq and Wistron), Taiwanese-owned factory in China (Quanta), or South Korean-owned factory in China (Samsung)</td>
</tr>
<tr>
<td>Keyboard</td>
<td>Japanese company in China (Alps), or Taiwanese-owned factory in China (Sunrex and Darfon)</td>
</tr>
<tr>
<td>LCD</td>
<td>South Korea (Samsung, LG Philips LCD), Japan (Toshiba or Sharp), or Taiwan (Chi Mei Optoelectronics, Hannstar Display, or AU Optronics)</td>
</tr>
<tr>
<td>Wireless Card</td>
<td>Taiwan (Askey or Gemtek), American-owned factory in China (Agere) or Malaysia (Arrow), or Taiwanese-owned factory in China (USI)</td>
</tr>
<tr>
<td>Modem</td>
<td>China (Foxconn), or Taiwanese company in China (Asustek or Liteon)</td>
</tr>
<tr>
<td>Battery</td>
<td>American-owned factory in Malaysia (Motorola), Japanese company in Mexico, Malaysia, or China (Sanyo), or South Korean or Taiwanese factory (SDI and Simplo)</td>
</tr>
<tr>
<td>Hard Disk Drive</td>
<td>American-owned factory in Singapore (Seagate), Japanese-owned company in Thailand (Hitachi or Fujitsu), or Japanese-owned company in the Philippines (Toshiba)</td>
</tr>
<tr>
<td>CD/DVD</td>
<td>South Korean company with factories in Indonesia and Philippines (Samsung), Japanese-owned factory in China or Malaysia (NEC), Japanese-owned factory in Indonesia, China, or Malaysia (Teac), or Japanese-owned factory in China (Sony)</td>
</tr>
<tr>
<td>Notebook Carrying Bag</td>
<td>Irish company in China (Tenba), or American company in China (Targus, Samsonite, and Pacific Design)</td>
</tr>
<tr>
<td>Power Adapter</td>
<td>Thailand (Delta), or Taiwanese-, South Korean-, or American-owned factory in China (Liteon, Samsung, and Mobility)</td>
</tr>
<tr>
<td>Power Cord</td>
<td>British company with factories in China, Malaysia, and India (Volex)</td>
</tr>
<tr>
<td>Removable Memory Stick</td>
<td>Israel (M-System), or American company with factory in Malaysia (Smart Modular)</td>
</tr>
</tbody>
</table>

Source: Booz Allen Hamilton and DoD
Everybody has a supply chain except for god

We are all in this together

• The number of breaches attributed to business partners remained flat since 2007

• At the same time the number of breaches attributed to external threat increased tenfold, from roughly 100 (same as partners) to over 1000 in 2013

• Proportion of all breaches attributed to business partners decreased since 2007 to a negligible number

• Proportion of all breaches attributed to external threat increased from approximately 40% to about 90%

http://www.verizonenterprise.com/DBIR/2014/
Standards and practices are there to help figure it out.

**Government**
- Comprehensive National Cybersecurity Initiative
- DoD ICT SCRM Key Practices Document
- The President's International Strategy for Cyberspace
- PMOs developed in DOJ and DOE
- DHS ICT Supply Chain Exploits Frame of Reference

**Industry**
- DHS Vendor Procurement Language
- SAFECODE Software Supply Chain Integrity papers
- IEC 62443-2-4 – Requirements for IACS Solution Suppliers
- SAE Counterfeit Electronic Parts Avoidance series (SAE AS5553, SAE AS6081, etc.)
- Open Trusted Technology Framework and Conformity Assessments

**Timeline**
- 2008: Cyberspace Policy Review
- 2009: NIST IR 7622
- 2010: DoD ICT SCRM Key Practices Document
- 2011: The President's International Strategy for Cyberspace
- 2012: PMOs developed in DOJ and DOE
- 2013: DHS ICT Supply Chain Exploits Frame of Reference
- 2014: Open Trusted Technology Framework and Conformity Assessments

**Additional Resources**
- DHS Vendor Procurement Language
- SAFECODE Software Supply Chain Integrity papers
- IEC 62443-2-4 – Requirements for IACS Solution Suppliers
- SAE Counterfeit Electronic Parts Avoidance series (SAE AS5553, SAE AS6081, etc.)
- Open Trusted Technology Framework and Conformity Assessments