Information and Communication Technology (ICT) Supply Chain Security – Emerging Solutions

Nadya Bartol, CISSP, CGEIT
UTC Senior Cybersecurity Strategist
Agenda

• Problem Definition
• Existing and Emerging Practices
• Ten Key Questions
• Summary and Questions
Agenda

• Problem Definition
• Existing and Emerging Practices
• Ten Key Questions
• Summary and Questions
What is ICT Supply Chain Risk Management?

- Information and Communication Technology (ICT) products are assembled, built, and transported by geographically extensive supply chains of multiple suppliers.
- Acquirer does not always know how that happens, even with the primary supplier.
- Not all suppliers are ready to articulate their cybersecurity and cyber supply chain practices.
- Abundant opportunities exist for malicious actors to tamper with and sabotage products, ultimately compromising system integrity, reliability, and safety.

Acquirers need to be able to understand and manage associated risks.

Source: Nadya Bartol, ACSAC Case Study, December 2010
How does this look?

From *The World Is Flat by Thomas Friedman*

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 (Compal 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
What are the risks?

- Intentional insertion of malicious functionality
- Counterfeit electronics
- Poor practices upstream
Intentional insertion of malicious functionality

Problem Definition
Counterfeit Electronics

Problem Definition

Counterfeit Component

Provider/Integrator

Extra Features

Poor Performance

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Counterfeit Component

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier

Supplier
Poor practices upstream

Problem Definition

- Poor coding practices
- Supplier
- Supplier
- Supplier
- Supplier
- Poor quality
- Supplier
- Supplier
- Supplier
- Supplier
- Supplier
- Provider/Integrator
- Poor Performance
This may impact reliability and safety for years.

Problem Definition

- Poorest quality
- Poor coding practices
- Supplier
- Counterfeit Component
- Virus
- Supplier
- Extra Features
- Provider/Integrator
- Poor Performance
- Counterfeit Component
- Supplier
- Backdoor
- Supplier
- Supplier
- Supplier
- Supplier
- Supplier
Some History

US government reports on globalization, supplier risk, offshoring, foreign influence in software, and microelectronics

US Comprehensive National Cybersecurity Initiative Stood Up

US Comprehensive National Cybersecurity Initiative Stood Up

2007-2009 2008 2009

2009

2010

2011

2011

2012

2013

1999-2006

European reports on robustness of communications infrastructures and IT supply chain risks

Stuxnet

ENISA study on supply chain integrity

Telvent hacked

US House Intelligence Committee Huawei and ZTE report released

NDAA 2013 Cyber EO PPD 21

Mandiant Report

Problem Definition

© 2012 Utilities Telecom Council
Agenda

• Problem Definition
• Existing and Emerging Practices
• Ten Key Questions
• Summary and Questions
Existing and Emerging Practices

Government

- Comprehensive National Cybersecurity Initiative Stood Up
- DoD ICT SCRM Key Practices Document
- The President’s International Strategy for Cyberspace
- DHS ICT Supply Chain Exploits Frame of Reference

2008
- Cyberspace Policy Review
- DHS Vendor Procurement Language

2009
- SAFECODE Software Supply Chain Integrity papers
- GAO Report

2010
- Open Trusted Technology Framework
- Common Criteria Technical Document
- ISF Supplier Assurance Framework

2011
- Energy Delivery Systems Procurement Language
- IEC 62443-2-4 – Industrial-process measurement, control and automation

2012
- NIST SP 800-161 PMOs developed in DOJ and DOE

2013
- SAE Counterfeit Electronic Parts Avoidance series (SAE AS5553, SAE AS6081, etc.)

Industry
Existing and Emerging Practices

Government

- Comprehensive National Cybersecurity Initiative Stood Up
- DoD ICT SCRM Key Practices Document
- The President’s International Strategy for Cyberspace
- GAO Report
- DHS ICT Supply Chain Exploits Frame of Reference

Industry

- DHS Vendor Procurement Language
- SAFECODE Software Supply Chain Integrity papers
- Open Trusted Technology Framework
- Common Criteria Technical Document
- ISF Supplier Assurance Framework
- IEC 62443-2-4 – Industrial-process measurement, control and automation
- Energy Delivery Systems Procurement Language

- SAE Counterfeit Electronic Parts Avoidance series (SAE AS5553, SAE AS6081, etc.)
Existing and Emerging Practices

Government

- Comprehensive National Cybersecurity Initiative Stood Up
- DoD ICT SCRM Key Practices Document
- The President’s International Strategy for Cyberspace
- GAO Report
- DHS ICT Supply Chain Exploits Frame of Reference

2008
- Cyberspace Policy Review
- DHS Vendor Procurement Language

2009
- SAFECodes Software Supply Chain Integrity papers

2010
- Open Trusted Technology Framework

2011
- Common Criteria Technical Document
- ISF Supplier Assurance Framework
- IEC 62443-2-4 – Industrial-process measurement, control and automation

2012
- Energy Delivery Systems Procurement Language

2013

Industry

- SAE Counterfeit Electronic Parts Avoidance series (SAE AS5553, SAE AS6081, etc.)
Existing and Emerging Practices

Government

- Comprehensive National Cybersecurity Initiative Stood Up
- DoD ICT SCRM Key Practices Document
- The President’s International Strategy for Cyberspace
- DHS ICT Supply Chain Exploits Frame of Reference
- NIST SP 800-161 PMOs developed in DOJ and DOE

Industry

- DHS Vendor Procurement Language
- SAFECODE Software Supply Chain Integrity papers
- Open Trusted Technology Framework
- ISF Supplier Assurance Framework
- IEC 62443-2-4 – Industrial-process measurement, control and automation
- Energy Delivery Systems Procurement Language
- SAE Counterfeit Electronic Parts Avoidance series (SAE AS5553, SAE AS6081, etc.)

2008 - 2013

Cyberspace Policy Review

Cyberspace Policy Review

Cyberspace Policy Review

Cyberspace Policy Review

Cyberspace Policy Review

Cyberspace Policy Review

Cyberspace Policy Review

Cyberspace Policy Review
Existing and Emerging Practices

Government
- Comprehensive National Cybersecurity Initiative Stood Up
  - DoD ICT SCRM Key Practices Document
  - The President’s International Strategy for Cyberspace
- Cyberspace Policy Review
- NIST SP 800-161 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
- Open Trusted Technology Framework
- Common Criteria Technical Document
- ISF Supplier Assurance Framework
- IEC 62443-2-4 – Industrial-process measurement, control and automation
- Energy Delivery Systems Procurement Language
- SAE Counterfeit Electronic Parts Avoidance series (SAE AS5553, SAE AS6081, etc.)
How do these standards help?

By answering the following key question:

• How should an organization manage security risks associated with acquiring ICT products and services?

AND

By providing a rich menu of items to chose from to

• Define your own processes for supplier management
• Ask your suppliers about their processes
Agenda

• Problem Definition
• Existing and Emerging Practices
• Ten Key Questions
• Summary and Questions
(1) What ICT assets and processes are critical to your business?

<table>
<thead>
<tr>
<th>Assets and Processes</th>
<th>ICT Products and Services</th>
<th>ICT Suppliers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network gear</td>
<td>90%</td>
<td>10%</td>
</tr>
<tr>
<td>Control systems</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>Servers</td>
<td>50%</td>
<td>25%</td>
</tr>
<tr>
<td>Database software</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>Laptops</td>
<td>100%</td>
<td></td>
</tr>
</tbody>
</table>
(2) Have you defined what security you want?

<table>
<thead>
<tr>
<th>Critical Assets</th>
<th>Security Requirements</th>
<th>Validated Against Standards and Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network gear</td>
<td>90%</td>
<td>• Confidentiality</td>
</tr>
<tr>
<td></td>
<td>10%</td>
<td>• Integrity</td>
</tr>
<tr>
<td>Control systems</td>
<td>50%</td>
<td>• Availability</td>
</tr>
<tr>
<td></td>
<td>50%</td>
<td></td>
</tr>
<tr>
<td>Servers</td>
<td>50%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>25%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>25%</td>
<td></td>
</tr>
<tr>
<td>Database software</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>Laptops</td>
<td>100%</td>
<td></td>
</tr>
</tbody>
</table>

...and can you use these requirements to negotiate security with your suppliers?
(3) How will you know that the supplier is doing what they said they will do?
(4) Has the supplier implemented a secure lifecycle?

- Security reviews are conducted throughout the lifecycle
- Developers are trained in secure coding practices
- Secure code repositories are used
- Supplier knows the origins of critical components
- Lifecycle stops until critical weaknesses are fixed
- Supplier heard of best practices (e.g., OWASP or Microsoft SDL)
(5) How will your data be protected when it is exchanged with the supplier? With the acquirer?
(6) How will you and the supplier communicate vulnerabilities? You and the acquirer?

- Disclose or not disclose?
- How to disclose?
- Who will fix?
- If cannot fix, who will remediate?

New Vulnerability
(7) How will you and the supplier communicate about incidents? You and the acquirer?

- Disclose or not disclose?
- How and what to disclose?
- How to minimize the impact to both?

Incident or Breach

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive</td>
<td></td>
</tr>
<tr>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Personally Identifiable Information</td>
<td></td>
</tr>
<tr>
<td>Intellectual Property</td>
<td></td>
</tr>
<tr>
<td>Publicly Releasable</td>
<td></td>
</tr>
</tbody>
</table>
Ten Key Questions

(8) How will you (acquirer and supplier) protect yourself for the entire life span of the system?

Development/Engineering

Operations/Maintenance

Supplier out of business

Support discontinued

Parts no longer available

Retirement/Termination
(8) How will you (acquirer and supplier) protect yourself for the entire life span of the system?
(8) How will you (acquirer and supplier) protect yourself for the entire life span of the system?

- Provisions for hardware and software to be available in the future for maintenance and sustainment
- Software escrow
- Buy parts for the future
- Approved resellers and disposers
(9) How will this relationship be terminated securely?

<table>
<thead>
<tr>
<th>Development/Engineering</th>
<th>Operations/Maintenance</th>
<th>Retirement/Termination</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sensitive</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidential</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personally Identifiable Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intellectual Property</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Publicly Releasable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
(10) How will the people know what to do?

### Ten Key Questions

#### Points of Contact

<table>
<thead>
<tr>
<th>Supplier 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplier 2</td>
<td></td>
</tr>
<tr>
<td>Supplier 3</td>
<td></td>
</tr>
<tr>
<td>....</td>
<td></td>
</tr>
<tr>
<td>Supplier X</td>
<td></td>
</tr>
</tbody>
</table>

#### Awareness for All Involved

- Acquisition/procurement
- Legal
- Developer/engineer
- Delivery/shipping/receiving
- Executives
- Others?
(10) How will the people know what to do?

Points of Contact

| Supplier 1 | Supplier 2 | Supplier 3 | ..... | Supplier X |

Awareness for All Involved

- Acquisition/procurement
- Legal
- Developer/engineer
- Delivery, shipping, receiving
- Executives
- Others?
(10) How will the people know what to do?

Points of Contact

| Supplier 1 | Frodo Baggins |
| Supplier 2 | Harry Potter |
| Supplier 3 | Peter Pan |
| .....     | .....        |
| Supplier X| Cinderella   |

Awareness for All Involved

- Acquisition/procurement
- Legal
- Developer/engineer
- Delivery, shipping, receiving
- Executives
- Others?

What about your suppliers?
Agenda

- Problem Definition
- Examples
- Existing and Emerging Practices
- Ten Key Questions
- Summary and Questions
In Summary

- ICT supply chain concerns are at the heart of today’s technology acquisition

- Acquirer practices and supplier practices are equally critical

- You may already have these practices somewhere in your organization

- Use ten basic questions together with existing standards and practices to get started
Contact Information

• Nadya Bartol
  nadya.bartol@utc.org