Cyber Supply Chain Risk Management: Threats and Mitigation Strategies

J. Philip Craiger, Ph.D., CISSP
Professor of Cybersecurity
Embry-Riddle Aeronautical University
&
Co-Principal Investigator NCyTE

Presentation for HI-TEC 2021
NCyTE Center and this material is based upon work supported by the National Science Foundation under Grant #1902329.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.
Overview

- What is the ‘supply chain?’
- What are the phases of the supply chain?
- Why and where is the supply chain susceptible to malign actors?
- What is ‘cyber supply chain risk management?’
- Current and emergent laws and regulations
- NCyTE YouTube series
The supply chain problem: Maersk incident
Maersk cyber incident

- 800 seafaring vessels accounting for 1/5 of the entire world's shipping capacity
- Ransomware infected a single computer on Maersk's network
- Infection spread 170 offices around the world
  - 4,000 servers, 45,000 PCs, and 2,500 applications over a ten-day period
- Port terminals in the United States, India, Spain, and the Netherlands – all run by Maersk – experienced massive disruptions
The effect

• Cost $10 billion dollars
• Components and products needed for commerce were left stranded on the ships
• Affected companies, developers, suppliers, and customers
The Maersk incident was an example of a cyber supply chain attack.
“A supply chain is a network between a company and its suppliers to produce and distribute a specific product to the final buyer. This network includes different activities, people, entities, information, and resources.

The supply chain also represents the steps it takes to get the product or service from its original state to the customer.” (Investopedia)
What is the supply chain problem?

• The world is relying more and more on advanced hardware and software: information communication technologies (ICT)
  • ICT products include computers, networks, smartphones
  • Security cameras, game boxes, smart watches, Wi-Fi access points ...
  • Aircraft, ships, automobiles, trains, helicopters, subways ...

• ICT products are built on hardware containing hundreds or thousands of physical components

• The physical components and software that drive ICT products are typically sourced from a variety of sources

• Globalization of the marketplace means that those components and software can be sourced from dozens or hundreds of companies throughout the world
How Software Is Eating the Car

The trend toward self-driving and electric vehicles will add hundreds of millions of lines of code to cars. Can the auto industry cope?
Are the physical components and software “cybersecure?”
Have the products been designed and tested to ensure confidentiality, integrity, and availability?
Changing nature of supply chains

• Current and emergent technologies are composed of significantly more diverse, complex, and commercially available hardware components and software than any time in history.
• The supply chain for these technologies may involve sourcing from a hierarchy of suppliers, from prime contractors, to Tier 1, 2, 3 and Tier 4 subcontractors that provide hardware components, software, and services to upstream and downstream suppliers within the supply chain.
• Even lower-tier suppliers, often small- and medium-sized businesses, are reliant on a global supply chain network.
Adapted from Popick and Reed, 2013, with permission
If ICT products contain components and software that are sourced from multiple, changing, and diverse suppliers, how can we be sure that they are secure?
Where can supply chain attacks occur?
Phases of the supply chain
Phases of the supply chain
Phases of the supply chain
Phases of the supply chain

- Requirements
- Design
- Develop/Manufacture
- Testing
Phases of the supply chain

- Requirements
- Design
- Develop/Manufacture
- Testing
- Distribution
Phases of the supply chain

Requirements → Design → Develop/Manufacture → Testing → Distribution → Use/Maintenance
Phases of the supply chain

Requirements → Design → Develop/Manufacture → Testing → Distribution → Use/Maintenance → Disposal
Supply chain attacks can occur at any phase ...
Phases of the supply chain
The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America’s technology supply chain, according to extensive interviews with government and corporate sources.
The supply chain attack according to Bloomberg

• A Chinese military unit designed and manufactured microchips as small as a sharpened pencil tip.

• Some of the chips were built to look like signal conditioning couplers, and they incorporated memory, networking capability, and sufficient processing power for an attack.

• The microchips were inserted at Chinese factories that supplied Supermicro, one of the world’s biggest sellers of server motherboards.
The supply chain attack ...

• The compromised motherboards were built into servers assembled by Supermicro

• The sabotaged servers made their way inside data centers operated by dozens of companies

• When a server was installed and switched on, the microchip altered the operating system’s core so it could accept modifications

• The chip could also contact computers controlled by the attackers in search of further instructions and code
The chip essentially created a ‘backdoor’ to the server, allowing malign actors to connect to it, and alter or capture information.
Malign actors didn’t have to “hack” into the systems, they were provided a ‘built-in’ backdoor to the system
Where were these (allegedly) installed?

• Apple
• Amazon
• Central Intelligence Agency (drone operations)
• U.S. Navy warships
• Although the government conducted testing of the motherboards, and Bloomberg’s report was based on a year and half study from dozens of sources, several companies, including Supermicro, denied the claims

• Bloomberg stands by their report, and Apple no longer uses Supermicro boards, according to the report.
How can we mitigate potential cyber threats to the supply chain?
What is risk management?

• “Risk management is the ongoing process of identifying, assessing, and responding to risk.

• To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impacts.

• With this information, organizations can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk tolerance.”

Risk management regulations and guidelines to mitigate supply chain attacks
252.204-7012 Safeguarding covered defense information and cyber incident reporting.

As prescribed in 204.7304c, use the following clause:

Safeguarding Covered Defense Information and Cyber Incident Reporting (DEC 2019)

(a) Definitions. As used in this clause -

Adequate security means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

Compromise means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

Contractor attributional/proprietary information means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.
DFARS

• Defense Federal Acquisition Regulation Supplement.
• A contain requirements of law for federal contractors wishing to do business with the government.
• Businesses must meet the requirements, i.e., be “in compliance” in order to bid.
• 252.204-7012 deals with the security of unclassified defense information and cybersecurity incident reporting.
(b) **Adequate security.** The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered contractor information systems that are part of an information technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

   (i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.

   (ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.
(ii)

(A) The Contractor shall implement [NIST SP 800-171][1], as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

(B) The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

[1]: https://www.law.cornell.edu/cfr/text/48/252.204-7012
Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

COMPUTER SECURITY
NIST 800-171

• The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations.
• Provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident.
• The requirements apply to all components of nonfederal systems and organizations that process, store, and/or transmit CUI, or that provide protection for such components. Nonfederal systems and organizations.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
## Security families

<table>
<thead>
<tr>
<th>FAMILY</th>
<th>FAMILY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Media Protection</td>
</tr>
<tr>
<td>Awareness and Training</td>
<td>Personnel Security</td>
</tr>
<tr>
<td>Audit and Accountability</td>
<td>Physical Protection</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Identification and Authentication</td>
<td>Security Assessment</td>
</tr>
<tr>
<td>Incident Response</td>
<td>System and Communications Protection</td>
</tr>
<tr>
<td>Maintenance</td>
<td>System and Information Integrity</td>
</tr>
<tr>
<td>SECURITY REQUIREMENTS</td>
<td>NIST SP 800-53 Relevant Security Controls</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 3.1 ACCESS CONTROL

#### Basic Security Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Control</th>
<th>NIST SP 800-53</th>
<th>ISO/IEC 27001</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1</td>
<td>Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).</td>
<td>AC-2</td>
<td>Account Management</td>
<td></td>
</tr>
<tr>
<td>3.1.2</td>
<td>Limit system access to the types of transactions and functions that authorized users are permitted to execute.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018
The “Framework”

- “... a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks”

- The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes

- The “Framework” can be used by organizations in any sector or community: it enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience”

<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.SC</td>
<td>Supply Chain Risk Management</td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.AC</td>
<td>Identity Management and Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>
| **Supply Chain Risk Management (ID.SC):** | **ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders | **CIS CSC 4**  
**COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02  
**ISA 62443-2-1:2009** 4.3.4.2  
**ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2  
**NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9 |
|---|---|---|
| **ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process | **COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03  
**ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14  
**ISO/IEC 27001:2013** A.15.2.1, A.15.2.2  
**NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9 |
Why do we need so many regulations and guidelines?
Supply chains existed long before “cyber” became a problem, as such, cybersecurity was an ‘add-on’
Verification of compliance with regulations and guidelines was based on self-verification
“... to elevate the private sector’s focus on security, the Department has established a “Deliver Uncompromised” initiative focused on industry delivery of capabilities, services, technologies, and weapons systems that are uncompromised by our malign actors from cradle-to-grave.

It aims to establish security as a fourth pillar in acquisition, on par with cost, schedule, and performance, and to create incentives for industry to embrace security, not as a “cost center,” but as a key differentiator.

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

Version 1.0 | January 30, 2020
“While compliance with the DFARS is mandatory (as is compliance with NIST SP 800-171), in most cases, compliance with these regulations is based on the honor system.

The challenge with the honor system is that companies tend to be overly “optimistic” when asked about whether they are compliant.”
CMMC

• The CMMC is a unified standard for implementing cybersecurity across the defense industrial base (DIB)
  • Includes over 300,000 companies in the defense industrial base supply chain.

• Previously, contractors were responsible for implementing, monitoring and certifying the security of their information technology systems and any sensitive DoD information stored on or transmitted by those systems.
  • NOW: Contractors are responsible for implementing cybersecurity requirements, but now third-party assessments of contractors' compliance with certain mandatory practices is required.

CMMC

• CMMC is a unified cybersecurity standard for future DoD acquisitions

• CMMC Model v1.0 encompasses the following:
  • – 17 capability domains; 43 capabilities
  • – 5 processes across five levels to measure process maturity
  • – 171 practices across five levels to measure technical capabilities
17 Capability Domains (v1.0)

<table>
<thead>
<tr>
<th>Access Control (AC)</th>
<th>Incident Response (IR)</th>
<th>Risk Management (RM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Management (AM)</td>
<td>Maintenance (MA)</td>
<td>Security Assessment (CA)</td>
</tr>
<tr>
<td>Awareness and Training (AT)</td>
<td>Media Protection (MP)</td>
<td>Situational Awareness (SA)</td>
</tr>
<tr>
<td>Audit and Accountability (AU)</td>
<td>Personnel Security (PS)</td>
<td>System and Communications Protection (SC)</td>
</tr>
<tr>
<td>Configuration Management (CM)</td>
<td>Physical Protection (PE)</td>
<td>System and Information Integrity (SI)</td>
</tr>
<tr>
<td>Identification and Authentication</td>
<td>Recovery (RE)</td>
<td></td>
</tr>
</tbody>
</table>

CMMC Model with 5 levels measures cybersecurity maturity

- Level 1: Performed - Basic Cyber Hygiene
- Level 2: Documented - Intermediate Cyber Hygiene
- Level 3: Managed - Good Cyber Hygiene
- Level 4: Reviewed - Proactive
- Level 5: Optimizing - Advanced / Progressive
Summary

• ICT products are increasingly composed of COTS products/parts/services/hardware/software.
• Supply chains are increasingly complex, dynamic, unpredictable.
• Existing guidelines have relied on self-verification
• CMMC will require more rigor by using third-party testers.
Cyber Supply Chain Risk Management: Threats and Mitigation Strategies

J. Philip Craiger, Ph.D., CISSP
Professor of Cybersecurity
Embry-Riddle Aeronautical University
&
Co-Principal Investigator NCyTE

Presentation for HI-TEC 2021
Selected References


