Notices

© 2016 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This work was created with the funding and support of the U.S. Department of Homeland Security under the Federal Government Contract Number FA8721-05-C-0003 between the U.S. Department of Defense and Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN “AS IS” BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark of Carnegie Mellon University
Session Topics

- Foundations and background
- Threats to cyber-dependent supply chains
- Examples and case study
- Limitations of “outsourcing cyber risk” and management by contractual agreement
- Methods for managing resilient supply chains (focus on Covered Defense Information)
Learning Objectives

- Understand the fundamental concepts of managing risks to cyber-dependent supply chains

- Explore sources of risk in cyber-dependent supply chains

- Understand limitations of third party contracts

- Identify practical tools, technique, and methods for managing external dependencies and supply chain risk.

- Differentiate between operational resilience and traditional third-party performance requirements
Foundations
Foundation: CERT Resilience Management Model

“... the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents...”

- Presidential Policy Directive – PPD 21
  February 12, 2013

<table>
<thead>
<tr>
<th>Protect (Security)</th>
<th>Sustain (Continuity)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform (Capability)</td>
<td>Repeat (Maturity)</td>
</tr>
</tbody>
</table>
Cyber Resilience Review (CRR)

- Department of Homeland Security initiative to help critical infrastructure providers understand their operational resilience and ability to manage cyber risk
- Derived from the CERT Resilience Management Model (CERT-RMM)
- A review of the overall practice, integration, and health of an organization’s cyber security program
- The CRR allows an organization to
  - develop an understanding of process-based cyber security capabilities
  - develop meaningful indicators of operational resilience
  - improve its ability to manage cyber risk to its critical services and related assets
- 252 Assessments performed to date on version 2
CRR Overview

A structured assessment available as:

- a one day, facilitated assessment
- a self-assessment utilizing a freely available online version

Data is protected as PCII – Protected Critical Infrastructure Information

Data analysis is done anonymously, for example:

- Performance of an entire sector
- Relationships between practices and questions

<table>
<thead>
<tr>
<th>CRR Domains</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td>CM</td>
<td>Controls Management</td>
</tr>
<tr>
<td>CC M</td>
<td>Configuration and Change Management</td>
</tr>
<tr>
<td>VM</td>
<td>Vulnerability Management</td>
</tr>
<tr>
<td>IM</td>
<td>Incident Management</td>
</tr>
<tr>
<td>SC M</td>
<td>Service Continuity Management</td>
</tr>
<tr>
<td>RM</td>
<td>Risk Management</td>
</tr>
<tr>
<td>ED M</td>
<td>External Dependencies Management</td>
</tr>
<tr>
<td>TA</td>
<td>Training and Awareness</td>
</tr>
<tr>
<td>SA</td>
<td>Situational Awareness</td>
</tr>
</tbody>
</table>
Sector Level Analysis
NIST Cybersecurity Framework for Critical Infrastructure

Table 2: Function and Category Unique Identifiers

<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>AM</td>
<td>Asset Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>BE</td>
<td>Business Environment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GV</td>
<td>Governance</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RA</td>
<td>Risk Assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RM</td>
<td>Risk Management</td>
<td></td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>AC</td>
<td>Access Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AT</td>
<td>Awareness and Training</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DS</td>
<td>Data Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP</td>
<td>Information Protection Processes and Procedures</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PT</td>
<td>Protective Technology</td>
<td></td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>AE</td>
<td>Anomalies and Events</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CM</td>
<td>Security Continuous Monitoring</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DP</td>
<td>Detection Processes</td>
<td></td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>AN</td>
<td>Analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MI</td>
<td>Mitigation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IM</td>
<td>Improvements</td>
<td></td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RP</td>
<td>Recovery Planning</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IM</td>
<td>Improvements</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CO</td>
<td>Communications</td>
<td></td>
</tr>
</tbody>
</table>
Specific examples:

Breach of covered defense information (CUI) or other sensitive information

Tainted or counterfeit technology

Unintended or unknown functionality

Process failures – for example failure to identify or track sensitive information
Examples and short case study
Recent commercial sector third party data breaches

• Why you should care about granting control of your data to service providers
  • Selected breach incidents
    - Lowes (2014)
    - DoD TRANSCOM (2014)
    - HAVEX (2014)
    - AT&T (2014)
    - Target (2013)
    - New York State Electric and Gas (2012)
    - California Department of Child Support Services (2012)
    - Thrift Savings Plan (2012)
    - Epsilon (2011)
    - Silverpop (2010)
Case study: TRANSCOM
TRANSCOM target – military logistics capability

SASC identified fifty successful intrusions targeting TRANSCOM contractors between June 1, 2012 and May 30, 2013

Twenty intrusions attributed to “Advanced Persistent Threat”

Contractor targets:

- CRAF – Civil Reserve Air Fleet
- VISA – Voluntary Intermodal Sealift Agreement Program
Information sharing in TRANSCOM case

Intrusions/Cyber Events Known to U.S. Government
June 1, 2012 - May 31, 2013

- Known to FBI: 15
- Known to AFOSI: 11
- Known to DC3*: 8
- Known to DSS: 7
- Known to TRANSCOM: 1

Other
- Suspected APT
- APT
Importance of cooperation and managing the supplier set

Figure 6: Who identifies data breaches

Many organizations devote a disproportionate amount of time and money to detection methods that fall below the 1% mark.
Limitations to managing through contract requirements
Risk in external dependencies

“One caveat of outsourcing is that you can outsource business functions, but you cannot outsource the risk and responsibility to a third party. These must be borne by the organization that asks the population to trust they will do the right thing with their data.”

~Verizon 2012 Data Breach Investigations Report
Does your organization document security objectives in agreements with third parties?

- No: 25%
- Yes: 25%
- Partially: 50%

Does your organization include measures of security performance in agreements?

- No: 30%
- Yes: 56%
- Partially: 14%

Does your organization monitor compliance to security objectives in agreements?

- No: 14%
- Yes: 18%
- Partially: 68%

Is cybersecurity performance considered when selecting third parties?

- No: 14%
- Yes: 68%
- Partially: 18%
Senate Armed Services Committee Report

TRANSCOM incident reporting contract language was:

- Interpreted differently by contractors, for example to mean system intrusions where exfiltration or corruption of DOD information had been confirmed
- Required contractors to know which systems contain DOD information
- Requires contractors to recognize APT attacks
- Focused ONLY on the information asset (DOD information)

KEY POINTS:
- Contract language is “in the eye of the beholder”
  - Important contractor relationships require “care and feeding”
Limitations of contract requirements

Contracts *can* do the following:

- Allocate risk
- Drive behavior
- Define breach

Basic questions on contract clauses involving confidentiality or data integrity:

- How do we prove breach?
- How do we prove damages (in monetary terms)?
- If contract non-renewal is a remedy, is it realistic?
An approach to protection of Covered Defense Information
DFARS 252.204-7XXX (Revised December 20, 2015):

- Defense contractors have until December 2017 to provide adequate security for all covered defense information on covered contractor information systems.

- Covered defense information is:
  - Provided to the contractor by DoD or developed by the contractor, and is
    - Controlled Technical Information
    - Critical information (OPSEC related)
    - Export control related
    - Any other information identified in the contract.
DFARS Adequate Security

The implementation of controls in NIST Special Publication 800-171 “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations”

- 109 security controls, selected by evaluating NIST 800-53 controls against tailoring criteria

- Or alternate but equally effective security measures used to compensate for the inability to satisfy a particular requirement

An offeror may propose to vary from NIST 800-171 by submitting a written explanation of why a requirement is not applicable or how an alternative but equally effective measure is used to compensate. Deviations from NIST 800-171 become part of the contract
Application of NIST 800-171 Controls

- The control list is a highly relevant, useful set of controls to protect CDI

- Technology implementations may differ and change, meaning that not all controls will be applicable.

- Does not evaluate certain practices across the enterprise to sustain and institutionalize the controls

- A “point in time” assessment of control implementation may have a limited relevant period

- It does not address the contractors’ supply chain processes, other than flow down requirements
Elements of a Resilience Based Approach to Protecting Covered Defense Information

Focus on:

- Understanding and improving relevant organizational processes and capabilities
- Controls management for the protection of CDI
- Enterprise governance
Processes to protect CDI

Access Management
- Is CDI identified and tracked in an asset inventory?
- Are there policies and procedures for the proper marking of CDI?

Training and Awareness
- Is there insider threat training in place?
- Is the training evaluated for effectiveness?

Configuration and Change Management
- Are technology assets that store, process, or transmit CDI identified and inventoried?
- Is a change management process used to manage modifications to technology assets that store, process, or transmit CDI?
Sample practices to protect CDI

Incident Management
• Does the organization have a plan for managing incidents involving CDI?

Risk Management
• Are operational risks that could affect the confidentiality and integrity of CDI identified?
• Are risks tracked and a formal disposition (accept, transfer, mitigate, etc.) assigned?

Vulnerability Management
• Does the organization actively discover vulnerabilities affecting CDI?
Controls Management to Protect CDI

The purpose of Controls Management is to identify, analyze, and manage controls in an organization’s operating environment. Controls management helps an organization to build, analyze, and continuously update security controls.

• Do the organization's control objectives support the confidentiality of CDI?
• Are controls periodically analyzed to identify gaps where control objectives are not adequately satisfied?
Proposed control objectives focused on CDI

- Covered defense information is identified, inventoried, and marked in all contractor information systems.

- Third party (or service supply chain) relationships are formed and managed consistently with the need to protect CDI.

- Personnel are properly vetted, monitored, and trained to understand the risks of CDI disclosure and to protect CDI.

- Access to CDI is limited and managed.

- Events and incidents that potentially affect the confidentiality or integrity of CDI are detected, managed, and tracked to resolution.
Governance Focused on Protecting CDI

- Is there a policy for the protection of CDI?

- Is there management oversight focused on protecting CDI?

- Are activities to protect CDI periodically reviewed to ensure they are effective and producing intended results?
Governance matters . . .

Percentage of “yes” responses to external dependency management practices, correlated to planning, oversight, and measurement.

Planning

Management oversight

Measurement of effectiveness
| Access Management | 1. Is CDI identified and documented in an asset inventory? | Question Intent: To determine if covered defense information is inventoried.  
• The organization should inventory the CDI that it is responsible for protecting. This is so that it knows which information to protect and apply controls against.  
Criteria for “Yes” Response:  
• The organization has a process to inventory CDI in a documented listing or inventory.  
Criteria for “Incomplete” Response:  
• The organization inventories some CDI. |
| --- | --- | --- |
| 2. Are the physical locations of CDI (both within and outside the organization) documented in asset descriptions? [ADM:SG1.SP3] | Question Intent: To determine if the physical locations of CDI are documented in an asset inventory or similar repository.  
• Physical locations of information can be internal or external to the organization.  
• The location details should be sufficient enough to support the protection of the information.  
Criteria for “Yes” Response:  
• The organization documents the location of all identified CDI in the asset inventory or other documentation.  
Criteria for “Incomplete” Response:  
• The organization documents the location of some CDI. |
NIST Cyber Security Framework

The framework of the NIST CSF would be very useful for organizations protecting the confidentiality of CDI.

- NIST 800-171 introductory note:

  Framework for Improving Critical Infrastructure Cybersecurity

  Organizations that have implemented or plan to implement the NIST Framework for Improving Critical Infrastructure Cybersecurity can find in Appendix D of this publication, a direct mapping of the Controlled Unclassified Information (CUI) security requirements to the security controls in NIST Special Publication 800-53 and ISO/IEC 27001. Once identified, those controls can be located in the specific categories and subcategories associated with Cybersecurity Framework core functions: Identify, Protect, Detect, Respond, and Recover. The security control mapping information can be useful to organizations that wish to demonstrate compliance to the CUI security requirements in the context of their established information security programs, when such programs have been built around the NIST or ISO/IEC security controls. See [http://www.nist.gov/cyberframework](http://www.nist.gov/cyberframework).
Conclusions
# Traditional Contractor Management vs. Supply Chain Resilience

<table>
<thead>
<tr>
<th>Traditional Contractor Management</th>
<th>Supply Chain Resilience</th>
</tr>
</thead>
</table>
| Focus is on contract requirements and formal agreements | • Focus is on capabilities of acquirer and supplier  
  • Contracts and requirements are part of the approach |
| One organizational silo handles vendors and contractors | The right stakeholders in the organization have input into the process |
| Contractor controls are assessed at a single point in time | • The risk is continuously managed  
  • Assessments include the institutionalization of processes (policy, management, measurement) |
Bottom line, what are we suggesting?

Contractual requirements are not enough for hard supply chain problems and critical relationships.

Specific controls and security technology are very important, but are one part of an organization’s overall capability to manage risk.

Enterprise governance practices are a good predictor of program completeness and “stickiness” . . . institutionalization.

Fostering a climate where information about capabilities and processes is shared - in addition to threat and incident information – would be helpful.
Questions?
Contact Information

Presenter / Point of Contact
John Haller
CERT program – SEI
Telephone: +1 412-268-6648
Email: jhaller@cert.org

Web
https://www.dhs.gov/topic/cybersecurity
www.cert.org/resilience