Software & Supply Chain Assurance: Enabling Enterprise Resilience through Security Automation, Software Assurance, and Supply Chain Risk Management

Joe Jarzombek, PMP, CSSLP
Director for Software & Supply Chain Assurance
Cyber Security & Communications
US Department of Homeland Security
Risk Management (Enterprise ↔ Project): Shared Processes & Practices ↔ Different Focuses

► Enterprise-Level:
  - Regulatory compliance
  - Changing threat environment
  - Business Case

► Program/Project-Level:
  - Cost
  - Schedule
  - Performance

Who makes risk decisions / trades?
Who “owns” residual risk from tainted/counterfeit products?

* “Tainted” products are those that are corrupted with malware, or exploitable weaknesses & vulnerabilities that put users at risk.
ICT Supply Chain Exploitation

Toward a Common Frame of Reference for SwA & SCRM
Increased risk from supply chain due to:

- Increasing dependence on commercial ICT for mission critical systems
- Increasing reliance on globally-sourced IT hardware, software, and services
  - Varying levels of development & outsourcing controls
  - Lack of transparency
- Residual risk passed to end-user enterprise
  - Counterfeit products
  - Tainted products with malware, exploitable weaknesses and vulnerabilities
- Growing technological sophistication among our adversaries
  - Internet enables adversaries to probe, penetrate, and attack us remotely
  - Supply chain attacks can exploit products & processes throughout the lifecycle
Who is susceptible to supply chain exploitation?

- Banking and Finance
- Defense Industrial Base
- Energy
- Government Facilities
- Healthcare and Public Health
- Information and Communications Technology
- Nuclear Power
- Transportation
Where is DHS being pulled?

1. Protect Critical Infrastructure

1.1 Build partnership with private sector telecomm and IT companies to address SCRM (DHS)

1.3 Augment USG procurement of ICT equipment and services, to give USG system owners authority to require SCRM in response to emerging threats (GSA)

1.5 Consider new legislative authorities to regulate SCRM across dependent sectors (DOD & DOC)

1.6 Develop multi-tiered, standards-driven approach to standards-based risk management frameworks for SCRM (NIST & DHS & FCC)

1.7 Fund transition of critical technologies into domestic, sustainable production capabilities (OSTP & DPAC)

2. Bridge Security/Acquisition Gaps

2.1 Develop frame of reference for common discussion of SCRM threats, exploits, acquisition gaps, security measures. Develop and pilot analytic processes for evaluating SCRM.

2.2 Develop SCRM analytic tools for implementing SCRM consistently across D/As (including domain specific acquisition support, text analytics, risk-based decision support, forensics, control languages, standard messaging formats)

2.3 Track successful implementations of SCRM for promulgation of cost-effective, best practices

2.4 Support the development of SCRM policies, procedures, and governance for the implementation and monitoring of SCRM across civilian D/As

2.5 Develop operations for detection, forensics, incident response in collaboration with US-CERT and the NCCIC

2.6 Build relationships with acquisition groups and pilot SCRM tools, evaluate success, and continuously improve
Supply Chain Exploit Frame of Reference

- Complex, emerging supply chain risks
- Diverse, emerging policies, standards, best practices

We need a common language to describe supply chain exploitation, so that:

1. **Greater customization** of security controls (to reduce implementation costs)
2. **Better collaboration** across partners (to improve effectiveness of security activities)
Exploit Techniques

Production/Integration
Environmental Weaknesses

Vulnerable Systems

Exploits and weaknesses vary across systems, domains of custody, and phase of the system lifecycle.
(1) Common Language Example

- **Concept Develop**
- **Produce**
- **Utilize**
- **Support**
- **Dispose**

**Phase of System Lifecycle**

**Domain of Custody**
- Within Trusted Custody of Producer
- Transit or En-Route Storage
- Within Trusted Custody of Acquirer

**Exploit Technique**

1. Steal design of lab from contractor
2. Examine discarded copier
3. Alter copier to stenograph data to cover sheet
4. Coerce contracted maintenance to provide recycled cover sheets
5. Decipher cover sheets for intellectual property

**Knowledge**
- Knowledge of lab equipment
- Knowledge of delivery process
- Need for insider data
- Use Stolen IP
## (2) Countermeasure Prioritization

**Mitigations** (linked to Exploits and Weaknesses)

**Indicators** (of Exploits or Weaknesses)

**Basis for Prioritization of Mitigations**

### Mitigations and Indicators vary across systems, domains of custody, and phase of the system lifecycle.

<table>
<thead>
<tr>
<th>Individual Exploit Indicators</th>
<th>Company Exploit Indicators</th>
<th>Marketplace / Country Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized Activity</td>
<td>Failed/Inconsistent Aspects of Trusted Delivery</td>
<td>Movement of Manufacturing toward foreign ownership</td>
</tr>
<tr>
<td>Theft or Destruction</td>
<td>Foreign Associations</td>
<td>Government subsidies</td>
</tr>
<tr>
<td>Unexpected or Unusual Financial Activity or Interests</td>
<td>Unexpected or Unusual Financial Activity or Interests</td>
<td>Intelligence or Government Concerns</td>
</tr>
<tr>
<td>Overt Threats</td>
<td>Supply Chain Exploit Capabilities</td>
<td>News</td>
</tr>
</tbody>
</table>

### Preconditions

1. Identification and Authentication
2. Access Control
3. Configuration Management
4. Awareness and Training
5. Physical and Environmental Protection

### Distributed Enhancements

1. Establish security procedures
2. Establish alternative routes of information sharing

### Integrated Activities

1. Supply chain diversity
2. Develop countermeasures
3. Check for integration throughout process
4. Verify performance under stress

### Implementation/Assessment

1. Assess security of physical and logical implementation
2. Ensure that system remains operational during consequences of compromise
3. Examine system countermeasures
4. Implement updates without disrupting operations

### Operations/Maintenance

1. Prevent unnecessary information sharing
2. Prevent unavailability
3. Prevent degradation
4. Prevent failure

### Disposal

1. Ensure disposal prevents eavesdropping

---

**Homeland Security**

---

<table>
<thead>
<tr>
<th>Preconditions</th>
<th>Initiation</th>
<th>Development/Acquisition</th>
<th>Implementation/Assessment</th>
<th>Operations/Maintenance</th>
<th>Disposal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Identification and Authentication</td>
<td>1. Establish security procedures</td>
<td>1. Verify compliance with requirements</td>
<td>1. Assess security of implementation</td>
<td>1. Prevent degradation of system</td>
<td>1. Ensure disposal prevents eavesdropping</td>
</tr>
<tr>
<td>2. Access Control</td>
<td>2. Establish alternative routes of information sharing</td>
<td>2. Identify potential critical system components</td>
<td>2. Ensure that system remains operational during consequences of compromise</td>
<td>2. Prevent failure</td>
<td>2. Prevent unnecessary information sharing</td>
</tr>
</tbody>
</table>

---

**Secure Designs & Architectures**

**Testable Requirements**

**Reliable Provider Evaluations**

**Dependable Intelligence**

**Continuous Security**

---

**System Lifecycle**
(2) Countermeasure Prioritization EXAMPLE

- DHS draft SCRM Attachment to the 4300A Implementation Guide maps countermeasures to threats for analysis and selection of countermeasures that manage threats with a potential business impact.
Measure, Monitor, and Reprioritize Practices (Especially for Visibility, Understanding, and Control)

- To assess effectiveness of SCRM policy, it is necessary to identify measurable outcomes of SCRM, as well as the level of implementation.

- Measurement framework would serve as a foundation for understanding and improving SCRM practices.

Example Outcomes

<table>
<thead>
<tr>
<th>Risk Understanding</th>
<th>Interagency Partner Engagement</th>
<th>Contracting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidence in the quality of risk-related data</td>
<td>Ability to describe risks to senior business leaders</td>
<td>Firm knowledge of the controls portfolio in place at major contractors</td>
</tr>
<tr>
<td>Ability to use risk estimates in investment decisions</td>
<td>Ability to persuade interagency partners to make decisions based on risk information</td>
<td>Ability to describe the risk landscape of major contractors</td>
</tr>
<tr>
<td>Ability to identify significant new risks</td>
<td>Clear understanding of who holds responsibility for addressing control gaps</td>
<td>Contractors understand requirements necessary to comply with regulations</td>
</tr>
<tr>
<td>Ability to assess protection levels against newly identified threats</td>
<td>Interagency partners understand their responsibilities in managing risk</td>
<td>Contractors have confidence in ability to satisfy regulatory requirements and address gaps</td>
</tr>
<tr>
<td>Ability to effectively prioritize gaps for remediation</td>
<td>Interagency partners understand risk data</td>
<td>Contractors have confidence that information on configurations of controls is current and accurate</td>
</tr>
</tbody>
</table>

Example Levels of Implementation

- **Degree of Implementation**
  - Level 1: None
  - Level 2: 1 – 25%
  - Level 3: 26-50%
  - Level 4: 51-75%
  - Level 5: 76-100%

- **Maturity of Process**
  - Level 1: Focus only on known risks
  - Level 2: Focus on emerging risks on an ad-hoc basis
  - Level 3: Maintain a comprehensive list of risks that are consistently addressed
  - Level 4: Defined processes of identifying, defining, and incorporating emerging risks
  - Level 5: Monitor and optimize process for incorporating emerging risks

- **Intensity of Application**
  - Level 1: Little understanding of mission
  - Level 2: Basic understanding of mission
  - Level 3: Strong understanding of mission, but not priorities and strategic direction
  - Level 4: Strong understanding of mission with some sense of strategic direction
  - Level 5: Strong and broad understanding of process and well-developed sense of strategic goals
Examples of Transferable Technology/Resources:

- Test and Evaluation Processes
- Instantiation of BRANCH (Business Risk Analysis Clearing House)
SCRM Strategy

Engineer Tools

Identify & Respond

Outreach & Collaborate

Influence Policy

Develop Standards

Manage Supply Chain Risk

Policy decisions influence tool design
Tool design allows standards and policies to work
Standards are implemented by tools
Tools allow standards and policies to work

Standards are a foundation of good policy
Policies implement standards

4300A
ITAR QEG
D102-01

IR7622
SP800-53
SP800-161

US-CERT
NCCIC
I&A
DOJ

Text Analytics Capability Evals

Training
DOE&DOJ
FedVTE

NCCIC
NCIX
I&A
DOJ

NCCIC
NCIX
I&A
DOJ

Homeland Security

| 18 |
SCRM Systems Engineering Needs

1. A common language to describe supply chain exploits (1st rule of systems engineering – needed for SCRM)
2. Realistic method to prioritize mitigations
3. Phased implementation approach that includes monitoring/validating effectiveness of SCRM to discourage:
   – BOGSAT prioritization methods with no validation that cause “spending into oblivion” OR
   – “Hands-up” “cannot afford” responses of smaller components, yet interconnect into secured systems
4. Standard approaches for sharing measurable security plans to incorporate into provenance processes
(3) Need Measured, Phased Approach

Adapt NIST 800-39 Risk Management guidance:

1. the multitiered organization views and process elements must be elaborated upon for the integrated organization for SCRM (greater depth into supply chains), and

2. the risk management features must expanded to account for non-traditional IT operations (greater breadth to include development/acquisition operations and logistics).

Example Elaborations:

Tier One – Organization/Enterprise View

- Governance and Risk Executive includes integrated structure for IT, security, logistics, contracting, and so forth
- Risk Management Strategy frames supply chain threats and vulnerabilities (in both products and processes)
- Investment Strategies include secure replacement of exploitable modules

Tier Two – Mission/Business View

- Risk Awareness includes supply chain concerns, such as tainted and counterfeit products
- Enterprise/Infosec Architecture include development lifecycles and contracting details

Tier Three – Information System View

- Appropriate activities built in across lifecycle phases (e.g., development, acquisition, sustainment, operations)
(4) Security “Pipework”

MITRE, in collaboration with government, industry, and academic stakeholders, is improving the measurability of security through **registries** of baseline security data, providing standardized **languages** as means for accurately communicating the information, defining proper **usage**, and helping establish community approaches for standardized **processes**.

The other activities and initiatives listed here have similar concepts or compatible approaches to MITRE’s. Together all of these efforts are helping to make security more measurable by defining the concepts that need to be measured, providing for high fidelity communications about the measurements, and providing for sharing of the measurements and the definitions of what to measure.

Measurable security pertains at a minimum to the following areas:

- Software Assurance
- Supply Chain Risk Management
- Cyber Intelligence Threat Analysis
- Cloud Management
- Application Security
- Patch Management
- Configuration Management
- Cyber Threat Information Sharing
- Vulnerability Management
- Malware Protection
- Intrusion Detection System Assessment
- Incident Coordination
- Enterprise Reporting
- Remediation
Term Definitions

- **NIST IR 7622**
  - ICT Supply Chain Risk
    - Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. NIST SP 800-53 Rev 3: FIPS 200, adapted
  - ICT Supply Chain Risk Management
    - The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains.

- **CNSS Instruction 4009**
  - Risk is a measure of the *extent to which an entity is threatened* by a potential circumstance or event and is typically a function of 1) the *adverse impacts* that would arise if that circumstance or event occurs, and 2) the *likelihood* of its occurrence
  - Vulnerability is a *weakness that could be exploited* by a threat source
  - Threat is any *circumstance or event* with the potential to adversely impact organizational operations, assets, individuals, other organizations, or the Nation
  - Impact is the *magnitude of harm* that can be expected
Identifying DHS Concerns about how Supply Chain Exploits put users at risk

- SwA/SCRM Working Group session to collaboratively address how a frame of reference could assist:
  - Provide a common lexicon
  - Discuss countermeasures
  - Catalogue inspection/detection and analysis tools and techniques
SOFTWARE ASSURANCE FORUM

“Building Security In”

https://buildsecurityin.us-cert.gov/swa

Joe Jarzombek, PMP, CSSLP
Director for Software & Supply Chain Assurance
Cybersecurity & Communications
Department of Homeland Security
Joe.Jarzombek@hq.dhs.gov
(703) 235-5320
Cybersecurity and Communications

Responsible for enhancing security, resiliency, and reliability of the nation's cyber and communications infrastructure; actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm strategic assets.

Works to prevent or minimize disruptions to our critical information infrastructure in order to protect the public, the economy, government services, and overall security of the United States by supporting a series of continuous efforts designed to further safeguard federal government systems by reducing potential vulnerabilities, protecting against cyber intrusions, and anticipating future threats.

As the Sector-Specific Agency for the Communications and Information Technology (IT) sectors, CS&C coordinates national-level reporting consistent with the National Response Framework, and fulfills the mission through its five divisions:

- The Office of Emergency Communications (OEC)
- The National Cybersecurity and Communications Integration Center (NCCIC)
- Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR)
- Federal Network Resilience (FNR)
- Network Security Deployment (NSD)
A New Paradigm Presents a Problem

- The increased reliance on Bits and Bytes increases the risk of nontraditional attacks
  - Incidents of malicious cyber activity growing rapidly year over year
  - Counterfeit electronics entering government networks
Why it Matters

- **Industrial Espionage, National Security**
  - CFIUS

- **Criminal activity**
  - Operation b70
  - Microsoft’s Digital Crimes Unit disrupted more than 500 different strains of malware with the potential for targeting millions of innocent people.
Interdependencies Between Physical & Cyber Infrastructures: Convergence of Safety, Security and Dependability Considerations

-- Need for secure/resilient software applications

Software is a high risk component
Software Assurance Addresses Exploitable Software: Outcomes of non-secure practices and/or malicious intent

Software Assurance (SwA) is the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the life cycle.*

From CNSS Instruction 4009 “National Information Assurance Glossary” (26APR2010)

Exploitation potential of vulnerability is independent of “intent”

- **Defects**
- **Malware**
- **Exploitable Software**
  - Unintentional Vulnerabilities
  - Intentional Vulnerabilities

‘High quality’ can reduce security flaws attributable to defects; yet traditional S/W quality assurance does not address intentional malicious behavior in software

*Intentional vulnerabilities: spyware & malicious logic deliberately imbedded (might not be considered defects)