Supply Chain Security
How Do You Trust Your Suppliers? v1.2

Bill Jaeger, bjaeger@lenovo.com
October 27, 2017
About…

Bill Jaeger  Director, Security Architecture & DCG PSO

• Founding member Corporate & DCG Product Security Offices (PSO)

• Work with global product teams, industry partners, and customers to drive product security enhancements – achieving a number of “firsts” for Lenovo

• Support Product Security Incident Response Team (PSIRT)

• 25+ years solving complex security, operational, and technical challenges for government and commercial enterprises

• Historically well-cleared by US Government

• Author, speaker, inventor, CISSP, CSSLP
Overview

What is a supply chain?
How do you build a supply chain security program?
How do you determine which suppliers you can trust?

Supply Chain Security Background
Building a Trusted Supplier Program
Results and Lessons Learned
Supply Chain Security
Background
The Supply Chain

The Lifeblood of Organizations Large and Small

Definition*:
Supply Chain

• A system of organizations, people, activities, information, and resources involved in moving a product or service from supplier to customer.

• Supply chain activities involve the transformation of natural resources, raw materials, and components into a finished product that is delivered to the end customer.

* = https://en.wikipedia.org/wiki/Supply_chain
Business Drivers

Why Secure the Supply Chain?

• Reduce risk
• Build or maintain customer confidence
• Proactively address or reactively recover from supply chain issues
• Minimize counterfeits, fraud, interdiction, loss, vulnerabilities
• Regulatory compliance

Lenovo’s Trusted Supplier Program: Introduction

This Trusted Supplier Program was developed in response to increasing customer demand for transparency in the security of the hardware, firmware and software that is included in the products that they purchase. Customers have a heightened awareness regarding security when selecting suppliers. We need to be able to provide safety for our customers as well as to protect the Lenovo brand. The customers want to be able to trust that the computers that they purchase are authentic hardware, free of malicious code, and do not contain other security vulnerabilities that could be exploited.

The Trusted Supplier Program is intended to provide traceable and auditable documentation for security risk management over the entire breadth of the supply chain.

Building a Trusted Supplier Program
Where to Start?

A Sampling of Industry Standards and Frameworks

• NIST SP800-161 Supply Chain Risk Management Practices

• ISO/PAS 28000 Spec for Security Management Systems for the Supply Chain

• ISO/IEC 20243 Open Trusted Technology Provider Standard (O-TTPS)

• vBSIMM Vendor Building Security In Maturity Model
  – https://www.bsimm.com/about/bsimm-for-vendors.html

• Shared Assessments
  – https://sharedassessments.org/

• ISF Supply Chain Information Risk Assurance Process (SCIRAP)
Key Objectives
For Managing Supply Chain Risk

Identify potential risks to the supply chain

Protect
Build controls to help Protect the supply chain from risks

Detect
Detect issues early, providing time and options with which to respond

Respond
Respond quickly to mitigate the vulnerability or threat

Recover
Recover with minimal impact to customers
Trusted Supplier Program Elements

- Defined Scope
- Program Guide
- Supplier Onboarding Letter
- Supplier Security Questionnaire
- Supplier Security Agreement
- Security Assessments
- Trusted Supplier List
- Onsite Supplier Audits
- 3rd-Party Program Attestation
- Program Team
Defined Scope

**What Supply Chain Aspects Will Be Included?**

- **100% coverage may not be feasible**
  - Particularly for large supply chains

- **Prioritize based on criticality**
  - Most business critical
  - Largest (volume, $, other)
  - Perceived riskiest, fewest controls

- **Grow scope as program matures**
  - Crawl -> Walk -> Run

---

**Lenovo’s Scope: Intelligent Component**

- Software or firmware executable on any microprocessor
- Semiconductor device that has data processing ability
- Component or device that has internal memory
- Component or device that performs an input/output function

**Examples Covered Categories**

[Representative of Lenovo – Not Comprehensive]

- BIOS, BMC, Camera Modules, CPUs, Disk Drives, Display Panels, Fingerprint Sensors, Integrated Circuits, Keyboards, Memory, Mice, Motherboards, Network Cards, Network Switches, Optical Disk Drives, RF Modules, Software, Solid State Disks, TPMs, Video Cards, more…
- Manufacturing, Media Replicators
Program Guide & Supplier Onboarding Letter

Trusted Supplier Program “User Manuals” – Internal & External

• Program Guide
  – Comprehensive manual covering operational aspects of program
  – Potentially restricted to internal only

• Supplier Onboarding Letter
  – “Executive Summary” overview describing rationale, importance, coverage
  – Lets supplier know they’re not being singled out
  – Provided to suppliers as an intro

Lenovo’s Program Guide: Table of Contents

• Introduction
  • Definitions

• Trusted Supplier Program
  • Supplier Security Agreement
  • Trusted Supplier List
  • Supplier Security Questionnaire
  • Supplier Security Questionnaire Scoring
  • Supplier Security Audits
  • Supplier Security Audit Scoring
  • Offering Development Team Requirements
  • Supply Chain Issues Reporting Process
  • Security Program Document Revisions

• CVSS v3 Service Level Agreements
Supplier Security Questionnaire

Broad-scope Supplier Security Assessment

• Free form questionnaire
  – Covers scope of business and/or business line + products/services

• Completed by supplier

• Objective is to understand risks

• Responses drive risk evaluation

• Risk evaluation informs
  – Approve or Reject decision
  – Remediation actions, if any

Lenovo’s Supplier Security Questionnaire: Areas of Coverage

• General
  • Asset Management
  • Human Resources
  • Physical & Environmental
  • Communication & Operations Management
  • Access Control
  • Supplier Relationships
  • IT Acquisition, Development, & Maintenance
  • IT Security & Incident Management
  • Business Continuity Management
  • Standards & Legal Compliance

• Software, Firmware, & Mfg Test Software
  • Development Security Practices
  • Software / Firmware Security

• Hardware
  • Components & Counterfeit Prevention
  • Shipping & Containers
  • Material Incident Management, Investigation
Supplier Security Agreement

Contractual Agreement Defining Security Commitments

- The lynchpin of a successful Trusted Supplier Program
- Agreement execution
  - Easiest when signing new or renewing existing supplier contracts
  - Can be challenging to overlay upon existing supplier contracts
- Be flexible with details, but maintain overall principles
- Helpers
  - Scale (volume, $, ‘fame’, other)
  - Shared objectives
  - Current security events

Lenovo’s Supplier Security Agreement:
Areas of Coverage

- Definitions
- Security Specification
  - Minimize Vulnerabilities
  - Protect Data
  - Security Policies / Program
  - Business Continuity Plan
  - Breach Notification
  - Incident Response Capability
  - Vulnerability Fix SLA
- Program Requirements: Agree to…
  - Participate in Trusted Supplier Program
  - Answer Questionnaire & Update Annually
  - Provide Accurate Information
  - Intelligent Component Security Assessment
  - Compliance Audit
Security Assessments

*Find, Fix, and Validate*

• Let policy, risk dictate coverage

• Assessments are expensive
  – Leveraging supplier data may be viable, but confirm that the data is thorough, acceptable, and recent!

• Not one size fits all
  – Assessment types may vary based on supplier, product, or service
  – Some items may not be assessable or warrant assessment

• Healthy supplier relationships, shared goals ease remediation

---

**Lenovo Security Assessments:**

**Policy**

• Lenovo-branded products must be assessed
• Software shipping on Lenovo-branded products must be assessed (with certain exceptions)

**Areas of Coverage** (varies based on product)

• Binary extraction / Reverse engineering
• Composition analysis
• Dynamic analysis (configuration, malware, network, UEFI, web)
• Manual penetration test / ethnical hacking
• Fuzz testing
• Static code analysis
• Supplier-provided data review
**Trusted Supplier List**

*Source of Truth for Approved (and Rejected) Suppliers*

- **Availability to all to support procurement, development**

- **Supplier progression**
  - Candidate: to Approved or Rejected
  - Approved: to Rejected
  - Rejected: N/A

- **Candidate, Approved lists track**
  - Supplier, components, contacts, dates

- **Approved list also tracks**
  - Risk level, remediation needed
  - Maintain a separate, restricted access list of required remediation actions

---

**Lenovo’s Trusted Supplier List:**

**Supplier Status**

- **Approved:** 127
- **Candidate:** 80
- **Rejected:** 4

(Status as of 10/09/2017)

---

**Lenovo’s Supplier Status:**

**What Does It Mean?**

- **Approved:** Business - no restrictions
- **Candidate:** **Existing Supplier:** Business, but progress towards closure needed
  **New Supplier:** No business until Approved
- **Rejected:** No new business; draw down or cease existing business, with possible stop ship based on risk
Onsite Supplier Audits

*Trust, But Verify*

- **Physical review of questionnaire**
  - Primarily for manufacturing facilities
  - Also allows verification of physical security controls in office environments

- **Audit findings**
  - Acceptable or Needs Improvement
  - Supplier notified of result, any required remediation
  - If findings not remediated, finding feeds into risk evaluation and potential supplier move to Rejected list

---

**Lenovo’s Onsite Supplier Audits: Who Does It?**

- Supplier Quality Engineers (SQE)
- Procurement Engineers (PE)
- Manufacturing Engineers (ME)
- Security Subject Matter Experts
3rd-Party Program Attestation

*Provably Secure – Independent 3rd-party Attestation*

• It’s optional
  – Do it if it’s the right thing for your business; it may not be

• Why do it?
  – Help to bootstrap program
  – Provide assurance to customers, stakeholders, and to you!
  – Use as a competitive differentiator

Lenovo’s 3rd-Party Program Attestation:

**Conclusion**

“Chain Security believes that Lenovo’s implementation of the … Trusted Supplier Program … meet[s] or exceed[s] industry standards from a supply chain and product development security perspective and likely are at or above the level of its peers, including companies that are headquartered in the United States and currently provide products to the U.S. Government.”

08/2016
**Program Team**

*It Takes a Village for a Large Organization*

**Buildout**
- Executive support is critical, with formal policy chartering program even better
- Legal, Procurement are key partners

**Operation**
- Build supplier enrollment into procurement process
- Use program advocacy, training, road shows to drive adoption – this is both useful and needed with large and/or global procurement organizations
- A vigilant, dedicated, and firm Program Manager is needed for success

---

**Lenovo’s Program Team:**

**Who’s On The Extended Team?**

- Program Manager
- Legal
- Procurement / Global Commodity Managers
- Offering Development Team Leads
- Security Subject Matter Experts
- Penetration Testers
- Product Security Incident Response Team (PSIRT)
- Supplier Quality Engineers (SQE)
- Procurement Engineers (PE)
- Manufacturing Engineers (ME)
Results and Lessons Learned
Our Trusted Supplier Program Journey

By the Numbers

~2.25 Years
Since we started our Trusted Supplier Program

127 / 80 / 4
Approved / Candidate / Rejected suppliers

124 / 3
Low / Moderate Risk Approved suppliers

210
Questions in our Supplier Security Questionnaire

124*
Total security assessments performed over the past year (by Lenovo Data Center Group)

12*
3rd-party security assessments performed over the past year (by Lenovo Data Center Group)

* = Many security assessments cover multiple Intelligent Components

Statistics as of 10/09/2017
Lessons Learned [1/2]

Building a Trusted Supplier Program Isn’t Easy, But…
• It has proven vital to reducing supply chain risk
• It has improved supplier security for the benefit of all

Involving Supplier Business Contacts in Enrollment
• Business contacts can be a motivated advocate
• Agreement can be challenging when working solely with legal

Automate and Database…
• Spreadsheets and file systems are difficult to scale
• To enable better metrics, reporting, and analysis

Suppliers are Surprised When…
• They begin to understand that we are serious about our Trusted Supplier Program
• They don’t comply and are added to the Rejected list
Lessons Learned [2/2]

Security Assessments…
• Do identify weaknesses and vulnerabilities
• Open Source hygiene appears to be a near-universal challenge

Supplier Security Agreement…
• Vulnerability fix commitment and SLA helps in some cases
• Raises awareness, establishes dialog, and uncovers shared security goals in others

Trusted Suppliers…
• Have control of their supply chain and can prove it
• Will contractually commit to transparency and reasonable security obligations

Concerned Customers Want…
• Suppliers to demonstrate control of their supply chain
• Deliver upon commitments
Category: Sometimes Suppliers Write the Darndest Things...

$1 Insurance

What controls are in place to protect information assets based upon their security classification?

$2

No, we usually use paper files

Does your company have a policy or procedure on the use of encryption for the protection of information?

$5

No, but if have the heavy thing we will call 110

Are there policies or procedures in place that define when to contact internal security personnel or law enforcement?
Thank You