Beyond the XBOM: Holistic Supply Chain Risk Management

ACSAC 2023
An Existential Introduction

Why am I here?

Who am I?

What have I done?
Two tech-tonic shifts

Rocky transition to multi-polarity

Provenance of data and tech
Paradox of Perennial Surprise

Clever girl
Securing technology demands trust in how it works and is created – and by whom

- Security depends on establishing trusted relationships.
- Developing trust in the supply chain requires an atomic understanding of the ecosystem.
- Data about dependencies in the supply chain creates transparency.
- Transparency minimizes the need for trust.

Managing supply chain risk expects an understanding of the suppliers, products, and ecosystem.
Technology Sector

- Information Technology
  - Hardware
  - Servers
  - Processors
  - Cloud services
  - Data centers

- Software
  - Operating systems
  - Compilers and editors
  - Drivers and dependencies
  - Open-source scripts and packaged software
  - Repository engines, testing suites, and CI/CD tools

- Operational Technology
  - SCADA
  - DCS
  - PLC

- Data
  - Sensitive (SSN, DOB)
  - Financial (PCI)
  - Proprietary (IP)
  - Regulated (PHI)

- Devices
  - Medical
  - Sensors
  - Smart devices
  - Cameras

- Vendors
  - Outsourced
  - Consultants
  - Contractors
  - On site service providers
Supplier, Vendors, Third Parties, Oh My
Know the Flow
Which XBOM are we talking about?

Online radio station about post-apocalyptic Las Vegas

eXtensible Blockchain Object Model

Market identified code (stock ticker) for an Indian-listed company
The Genealogy of Development & Production Planning

- Engineering (eBOM)
- Manufacturing (mBOM)
- Sales or Service (SBOM)
- Pipeline (PBOM)
- Software (SBOM)
- Hardware (HBOM)
Elements of an XBOM

- Entry Points
  - APIs
  - Serverless
  - Protobuf Services

- Open Source
  - Dependencies
  - Licenses

- Confidential Information
  - Secrets
  - Sensitive data (PII, PCI, PHI)

- Data Management
  - Data Models
  - Data Access Objects
  - Protobuf Messages
  - GraphQL Objects

- Code Structure
  - Repositories
  - Code Modules
  - Technologies

- Kubernetes
  - Services
  - Deployments

- Infrastructure
  - Terraform
  - Dockerfile
Vendor Risk

Third Party Risk

C-SCRM

Security Rating Services

Software Supply Chain
Cyber Supply Chain Risk Spans Borders and Businesses
<table>
<thead>
<tr>
<th>Key Pain Points + Driving Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where and how does technology <em>across my supply chain</em> pose a risk to <em>my organization</em>?</td>
</tr>
<tr>
<td>Where and how does technology pose a risk to <em>my supply chain</em>?</td>
</tr>
<tr>
<td>Where and how does technology pose a risk to <em>an industry or ecosystem</em> which my organization depends on <em>but has no direct relationship with</em>?</td>
</tr>
</tbody>
</table>
Risk Management = Resource Allocation
Lessons for Transparency in Cyber Risk from Other Supply Chain Risks

- Incidents – detection: react
- Potential exposure – identification: minimize
- Impact – mitigation: monitor
- Performance - reporting: plan
Forced Labor
Foreign Ownership
Complex interdependencies make it impossible to ensure the security of all supply chain components and contributors.

Threat actors are economic, efficient, and entrepreneurial – and target weak links.

Third party exposure is not your fault, but it is your problem.
Additional Areas of Research

- Language / communications: third party vs. vendor vs. supply chain
- Complexity / complex systems: interactions between risks
- Security vs. risk: protecting vs. minimizing exposure
- Visibility: commercial has data, government has influence / incentives
Thank you!

Best way to find me: mwaltherpuri@exiger.com