MITRE’s System of Trust™
Framework and Community

Robert Martin
Cyber Solutions Innovation Center
MITRE Labs

Presented to the Software and Supply Chain Assurance Forum on 1 June 2023
Supply Chain Example – Consumer Clothing

- **Agriculture (natural fibers)**
  - Cotton
  - Wood
  - PRC
  - USA
  - India
  - Pakistan
  - Brazil
  - Uzbekistan

- **Trims**
  - PRC
  - India
  - Southeast Asia

- **Garments Manufacturer**
  - PRC
  - Bangladesh
  - Vietnam
  - India
  - Turkey

- **Distributor**
  - UK
  - EU
  - USA

- **Retailer**
  - UK
  - EU
  - USA

- **Consumer**

- **Yarn**
  - China
  - India
  - Southeast Asia
  - USA

- **Textiles**
  - PRC
  - India
  - USA
  - Turkey
  - South Korea

- **Chemicals (synthetics)**
  - USA
  - Southeast Asia
  - Middle East

- **Disposal**
Supply Chain Risk Areas

Natural Disasters and Hazards
- Floods
- Avalanche
- Drought
- Winds
- Heavy Rains
- Pandemics
- Earthquake
- Volcanoes
- Tornadoes
- Forest Fires
- Snow
- Thunderstorms
- Tsunamis

External Influences of the Supplier
- 3rd Party
- Risk Management

Quality Culture of the Supplier
- Financial Stability of the Supplier
- Organizational Stature of the Supplier
- Susceptibility of the Supplier

Maliciousness of the Supplier
- Organizational Security

Human Hazards
- Hijacking
- Corporate Corruption
- Traffic Congestion
- Civil Disruption
- Interdependent Supply Chains
- National Corruption

Attackers & Counterfeits
- Icons thanks to trajekx
Supply Chain Security (SCS) System of Trust (SoT)
“What Supply Chain Risks to Manage?”

SoT - a strategic, widely-adoptable, holistic, data-driven analysis platform to assess supply chain security risks

Address Chaos, Align & Organize
Simplify, Tailor & Use
Risk Categories

- Trust Aspects
- Supplier Risks
- Supply Risks
- Service Risks

**Basis of Trust**

**Risk Categories**

- **(RC-13) Supplier Financial Stability Risks**
  - Short-term Financial Health Risks
  - Financial Stewardship Risks
  - Adverse Market Factors
  - Long-term Financial Health Risks
  - Foreign Financial Obligations

- **(RC-76) Supplier Organizational Security Risks**
  - Technical Operations Risks
  - Cyber Threat Intelligence Risks
  - Security Training Deficiencies
  - Security Capabilities and Operations Risks
  - Cyber Threat Activity Risks
  - Security Governance and Compliance Risks

- **(RC-105) Supplier Organizational Effectiveness Risks**
  - Structural & Operational Instability
  - Geographical/Geopolitical Instability

- **(RC-7) Supplier Ethical Risks**
  - Association with Foreign Intelligence Service or Foreign Military Entity
  - Pattern of Criminal Behavior

- **(RC-6) Supplier External Influences**
  - Ownership and Control Risks
  - Foreign Business Relationship Risks
  - Adverse Corporate Influences

**Risk Categories**

- (RC-77) Supply Malicious Taint
- (RC-9) Supply Counterfeit
- (RC-8) Supply Hygiene Risks

- (RC-287) Service Quality Risks
- (RC-289) Service Resilience Risks
- (RC-286) Service Security Risks
- (RC-288) Service Integrity Risks
MITRE Supply Chain Security System of Trust Risk Areas* **

<table>
<thead>
<tr>
<th>(RC-1) Supplier Risks</th>
<th>(RC-2) Supply Risks</th>
<th>(RC-3) Service Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(RC-36) Supplier Vulnerability</td>
<td>(RC-9) Supply Counterfeit</td>
<td>(RC-29) Service Reliability Risk</td>
</tr>
<tr>
<td>(RC-40) Supplier Quality Culture Risks</td>
<td>(RC-10) Supply Counterfeit</td>
<td>(RC-29) Service Reliability Risk</td>
</tr>
<tr>
<td>(RC-42) Supplier Organizational Effectiveness Risks</td>
<td>(RC-11) Supply Counterfeit</td>
<td>(RC-29) Service Reliability Risk</td>
</tr>
<tr>
<td>(RC-34) Supplier Stability Risks</td>
<td>(RC-12) Supply Counterfeit</td>
<td>(RC-29) Service Reliability Risk</td>
</tr>
<tr>
<td>(RC-44) Supplier Use Risks</td>
<td>(RC-14) Supply Counterfeit</td>
<td>(RC-29) Service Reliability Risk</td>
</tr>
<tr>
<td>(RC-25) Supplier Ethical Risks</td>
<td>(RC-15) Supply Counterfeit</td>
<td>(RC-29) Service Reliability Risk</td>
</tr>
<tr>
<td>(RC-53) Subcontractor Supplier Chain Integrity Risks</td>
<td>(RC-16) Supply Counterfeit</td>
<td>(RC-29) Service Reliability Risk</td>
</tr>
<tr>
<td>(RC-48) Structural &amp; Operational Instability</td>
<td>(RC-17) Supply Counterfeit</td>
<td>(RC-29) Service Reliability Risk</td>
</tr>
<tr>
<td>(RC-49) Supply Chain Disruption Risks</td>
<td>(RC-18) Supply Counterfeit</td>
<td>(RC-29) Service Reliability Risk</td>
</tr>
<tr>
<td>(RC-50) Supply Chain Disruption Risks</td>
<td>(RC-19) Supply Counterfeit</td>
<td>(RC-29) Service Reliability Risk</td>
</tr>
<tr>
<td>(RC-51) Supply Chain Disruption Risks</td>
<td>(RC-20) Supply Counterfeit</td>
<td>(RC-29) Service Reliability Risk</td>
</tr>
</tbody>
</table>

* Supply Chain Security Top 78 Risk Areas Levels 1-3 ** System of Trust Expanding to Pharma, Food, and other types of Products

MITRE’s Supply Chain Security System of Trust™ [https://sot.mitre.org/](https://sot.mitre.org/)

© 2023 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-79
MITRE Supply Chain Security System of Trust Risk Catalog at 7 levels (aka Taxonomy/Vocabulary)
Taxonomy/Vocabulary

Data Model

Flexible Technology Stack

Risk Model Manager (RMM)

Piloting On-going

Export to Spreadsheet for “Offline” Assessment

Analytic Methods

© 2023 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-79
Tying together SoT and RMM
Tying together SoT and RMM
**Definition:**
- This risk considers how vulnerable to malicious activity a supplier may be due to the frequency and severity of externally observed cyber security incidents.

**Data Source:**
- Source: EDGAR, SEC, Wikipedia
- EDGAR database
- Enforcement actions: https://www.sec.gov/litigation/suspensions.shtml

**Risk Measures:**
- **High Risk:** Have there been reported and documented security issues, with three or more security incidents? Yes
- **Moderate Risk:** Have there been reported and documented security issues, with at least one to two security incidents? No
- **Low Risk:** Have there been no reported and documented security issues? No

4 issues found

- **Definition:**
  - This risk category considers the severity of external cyber security incidents.

- **Data Source:**

- **Risk Measures:**
  - High Risk: Has the company been affected by a cyber security incident?
  - Moderate Risk: Has the company been affected by a cyber security incident?
  - Low Risk: Has the company been affected by a cyber security incident?

(RC-105) Supplier Organizational Effectiveness Risks → (RC-538) → (RF-244) Supplier has frequently restructured through mergers & acquisitions

- **Rationale:**
  - Supplier has frequent restructure due to mergers and acquisitions.

- **Data Source:**

(RC-7) Supplier Ethics Risks → (RC-13) → (RC-26) → (RF-568) Supplier and/or key management personnel (KMP) have been targets of national or international criminal investigation

- **Rationale:**
  - A company is likely to be involved in illegal acts if KMP have been targets of criminal investigation.

- **Data Source:**

(RC-6) Supplier External Influences → (RC-5) → (RF-230) Supplier is wholly or partially owned by a foreign entity

- **Rationale:**
  - The likelihood that company operations are subject to antagonistic national interest is indicated by the potential allegiance of key partners and stakeholders.

- **Data Source:**
  - Source: Orbis BvD

- **Risk Measures:**
  - High Risk: Does this company have key stakeholder nationality of >= 15% from adversary or US Treasury watch list countries? No
  - Moderate Risk: Does this company have key stakeholder nationality of < 15% and > 5% from adversary or US Treasury watch list countries? No
  - Low Risk: Does this company have key stakeholder nationality of <= 5% from adversary or US Treasury watch list countries? Yes

None from adversary or US Treasury watch list country
(RC-4) Supplier Susceptibility

Supplier and Public Data Profile
Using 6 Risk Categories With 25 Risk Factors

7. External Cyber Security Incidents Risks
8. External Security Compromises/Breaches Risks

(RC-76) Supplier Organizational Security Risks
9. Intellectual property litigation involving supplier
10. Supplier sanction list status
11. Supplier and/or key management personnel (KMP) have been targets of national or international criminal investigation

(RC-7) Supplier Ethics Risks
12. Citizenship of key management personnel (KMP) and employees is in country/ies of concern

13. Ownership and Control Risks
15. Political Vulnerability
16. National Governance Risks
17. Geopolitical Instability
18. PEP Members in Corporate Leadership

(RC-13) Supplier Financial Stability Risks
1. Supplier may be unable to service its debts
2. Supplier has concerning inventory turnover rate
3. Supplier does not maintain adequate liquidity
4. Supplier has history of late payments
5. Supplier is not sufficiently profitable
6. Supplier falls behind its competitors in R&D investment level

(RC-105) Supplier Organizational Effectiveness Risks
19. Natural Disaster Risks
20. Geographic Concentration Risks
21. Mergers & Acquisition Frequency Risks
22. Operational Volatility Risks
23. Sustainability Risks
24. Corporate Ownership Risks
25. Diversity and Inclusion Risks
Risk Measures Bring Data to the Assessment of Risks
Pulling it Together

Potential Risk

Catalog of the different potential supply chain risks

Risk Factor

- Risk Measures
- Risk Measures
- Risk Measures
- Risk Measures
- Risk Measures
- Risk Measures
- Risk Measures

Data / information
Data / information
Data / information
Data / information
Data / information
Data / information
Data / information

© 2023 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-79
TIA SCS 9001, ISA/IEC 62443, , ISA/IEC 62443 or ISO/IEC 27001/2, ISO/IEC 27036, ISO/IEC 20243, ISO/IEC 27036, NIST CSF 1.1, NIST 800-37, NIST SP 800-161, NIST 800-53, NIST 800-171, CMMC Level 3-5 Assessment, ITAR, NDAA Section 889, TAPA FSR, NISP Facility Clearance, C-TPAP, SAE AS649, SAE AS6171, SOC 2 Type 2
Pulling it Together

Potential Risk

Catalog of the different potential supply chain risks

Risk Factor

Risk Measures

Data / information

Data / information

Data / information

Data / information

Data / information

Data / information

Data / information

Data / information

Site visit

Observe

SBOMs

Binaries

Vulnerability Assessment

Regression Testing

DAST

Claims from supplier about the supplies and the supplier

Direct measurement

Direct questioning

SCITT

web
Building up Sources of Insight about Supply Chain Risks
SoT Risk Model Manager Automation Technical Approach

Connecting to structured data
Where do I go to get the data about a particular risk factor?
How do I get access to the data?
SoT Risk Model Manager Automation Technical Approach

Connecting to structured data

What are the details for retrieving the data?
How do I interpret the data to determine if the risk is present?
SoT Risk Model Manager Automation Technical Approach

Connecting to structured data

Structure the answer and supporting data to send back to the RMM application.
SoT Risk Model Manager Automation Technical Approach

Connecting to structured data

Selector Implementer

Selector (Analytic) Implementation

Selector Lambda Implementations ECR Repository

API Gateway
Getting Access to RMM
https://sot.mitre.org/rmm/register.html
DoD Supply Chain Resiliency Work Group (DoD SCRM Taxonomy)

12 Categories & 124 subcategories
GOAL for use of SoT in Industry and Government…

Top-Level Concerns Vendor/Product A

- Malicious Taint
- Counterfeit
- Hygiene
- Service Security
- Service Quality
- Service Integrity
- Service Reliability
- External Influences
- Financial Stability
- Organizational Stature
- Quality Culture
- Susceptibility
- Organizational Security

Top-Level Concerns Vendor/Product B

- Malicious Taint
- Counterfeit
- Hygiene
- Service Security
- Service Quality
- Service Integrity
- Service Reliability
- External Influences
- Financial Stability
- Organizational Stature
- Quality Culture
- Susceptibility
- Organizational Security
System of Trust Risk catalog out for community review

MITRE'S System of Trust™ Body of Knowledge

REVIEW VERSION 1.2

January 17, 2022

© 2023 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-89
Examples of System of Trust Engagements

Executive Acquisition

Congressional Acquisition Groups
System of Trust (SoT)

SoT is not:

• a magical database of supply chain information
• a Supply Chain Risk Management approach
• a Logistics Management approach
• a Cyber Supply Chain Risk Management approach

SoT is:

• a compliment to SP 800-161 and other risk management guidance by enumerating the supply chain risks that may need to be managed
• a strategic, widely-adoptable, tailorable, data-driven analysis framework to promote assessment of the appropriate elements of a supply chain
• a nexus of assessment capabilities, standards, & information sources that is leverageable by MITRE, government and industry for repeatable, impactful analysis required for supply chain hygiene & due-diligence
System of Trust Components

A Language / Catalog of Supply Chain Risks w/ how to assess, contract, & COAs

Risk Model Manager
A Content Manager for the Risk Catalog

SoT Community
An external group working together on SoT

Public Website
An external place to share SoT capabilities

We Speak SoT™
SoT Compatibility
An Adoption Acceleration Program

SoT Capability
SoT Risk Model Manager for customers/projects
System of Trust Plans with Sponsors and the Community

- Assessment Capabilities for Sponsors, Industry and Academia
- Training Sponsors & Industry on the SoT methodology, content, and platform
- Standards and best practices oriented around SoT
- Evolving SoT Body of Knowledge with Domain SMEs to enhance Risk Factors
- Mapping SoT to Industry and Government standards and assessment mechanisms
- Active Feedback with communities on enhancements to SoT
- No-Cost Licensing Risk Model Manager tool & SoT content to Industry for integration in their own assessment practices and offerings
For more information...

https://www.cutter.com/offer/supply-chain-security-system-trust

