OTTF Supply Chain Security Concerns Survey Results

John Linford, Security Portfolio Forum Director, The Open Group

J.Linford@opengroup.org

https://www.linkedin.com/in/johndouglaslinford/

THE Open GROUP

THE OPEN GROUP TRUSTED TECHNOLOGY FORUM

Background

- OTTF completed update to O-TTPS, bringing it to V1.2
  - Published by The Open Group Sep. 2023
  - Published as ISO/IEC 20243-1:2023 and 20243-2:2023 Nov. 2023
- In updating Standards, the Forum began wondering about extending/expanding the O-TTPS
  - Cyber supply chain security
  - Business continuity management in the supply chain
- Determined survey would provide starting point for changes

Industry Input

Open Trusted Technology Forum

OTTF Public Input Portal

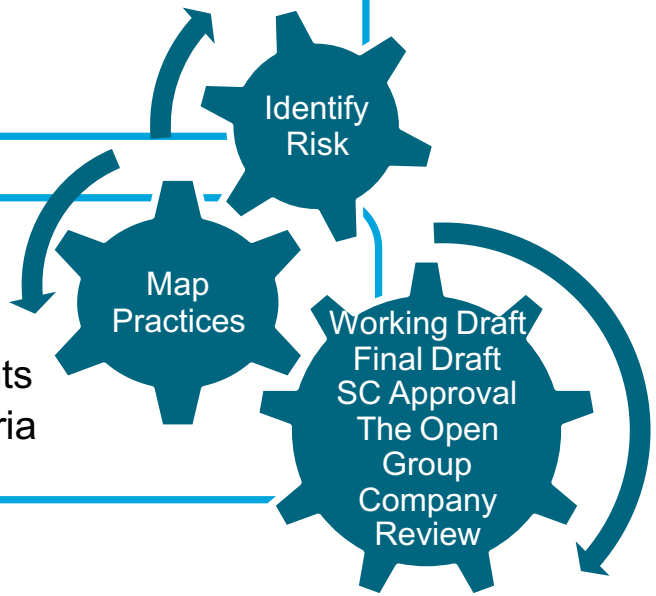
- Identify Industry Supply Chain Threats
- Solicit and Capture Industry Practices that Mitigate Threats
- Identify and Group Common Practices
- Comment on Practice Efficacy and Practicality

OTTF Framework (O-TTPF)

- Identify Best Practices
- Agree on Best Practice Attributes
- Adopts Practice(s) into Framework
- Document Practice(s) in Framework

O-TTPS Standard

- Validate Industry Supply Chain Threats
- Map O-TTF Practices to Risks
- Identify Best Practice Attribute Requirements
- Establish Accreditation Conformance Criteria



Technology Supply Chain Threat Matrix

	Taint			Counterfeit		
	Upstream	Provider	Downstream	Upstream	Provider	Downstream
Malware	✔	✔	✔			
Malicious code (masquerading as vulnerabilities)	✔	✔	✔			
Unauthorized Parts	✔	✔	✔	✔		
Unauthorized Configuration			✔			
Scrap/Substandard Parts				✔		
Unauthorized Production				✔		✔

Supply Chain Security Concerns Survey

Survey Structure

- Demographics
- Business Continuity Management in the Supply Chain
  - Third-Party Risk Management
    - Supply “Health”
    - Component and Service “Health
  - Special Topics in Supply Chain Business Continuity Management
- Cyber Supply Chain Security Concerns
  - Open-Source and Third-Party Software
  - Cyber Vulnerabilities
    - Acquired Products
    - Produced Products
  - SBOM
    - Use cases
    - Opportunities
    - Types
  - Special Topics in Cyber Supply Chain Security

Demographics Summary

- 38 unique respondents
- Organization size
  - 14 at 99 or fewer employees
  - 6 between 100 & 999 employees
  - 7 between 1,000 & 9,999 employees
  - 11 at 10,000+ employees
- Customer/Supplier or other
  - 19 customers
  - 14 suppliers
  - 2 consultants
  - 1 assessor
  - 1 accreditation body
  - 1 neither
- OEM vs Reseller (Answered “Supplier” in previous question)
  - 4 Integrator or value-add
  - 10 OEM
- Public vs Private
  - 13 private sector
  - 3 government
  - 19 blank
  - 1 DoD contractor
  - 1 FFRDC
  - 1 unclassified
- Topics most relevant
  - 4 BCM in supply chain
  - 18 cyber supply chain security
    - 3 completed BCM in supply chain at end of survey
  - 12 BOTH
    - 1 BOTH + “critical elements for space system”
    - 1 BOTH + “traceability & origin"
  - 1 “database product”
  - 1 “business intelligence”
  - 1 “security management”
  - 1 “origination of technology design”

Demographics Summary Cont.

- BCM in supply chain relevance (of 16 respondents)
  - 6 third-party risk management and service “health”
  - 4 third party risk management and supplier “health”
  - 6 both
    - 1 both + “geopolitical and disruption risks”
- Cyber supply chain security relevance (of 30 respondents)
  - 1 “Capability and Competency”
  - Cyber vulnerabilities in acquired products
  - 1 Cyber vulnerabilities in acquired products, Cyber vulnerabilities in produced products, “Cyber vulnerabilities in third-parties infrastructure”
  - 1 Cyber vulnerabilities in acquired products, Cyber vulnerabilities in produced products, Software Bill of Materials (SBOM)
  - 1 Cyber vulnerabilities in acquired products, Cyber vulnerabilities in produced products, Software Bill of Materials (SBOM), “Malicious content in supplied components”
  - 3 Cyber vulnerabilities in acquired products, Software Bill of Materials (SBOM)
  - 3 Cyber vulnerabilities in produced products
  - 1 Cyber vulnerabilities in produced products, Software Bill of Materials (SBOM)
  - 3 Open source and third-party software
  - 2 Open source and third-party software, Cyber vulnerabilities in acquired products
  - 6 Open source and third-party software, Cyber vulnerabilities in acquired products, Cyber vulnerabilities in produced products, Software Bill of Materials (SBOM)
  - 1 Open source and third-party software, Cyber vulnerabilities in acquired products, Cyber vulnerabilities in produced products, Software Bill of Materials (SBOM), “software build provenance”
  - 2 Open source and third-party software, Cyber vulnerabilities in acquired products, Software Bill of Materials (SBOM)
  - 1 Open source and third-party software, Software Bill of Materials (SBOM)

Business Continuity Management in the Supply Chain Results

17-19 respondents

Third-Party Risk Management: Supplier "Health"

Category	Blank	1 (not at all)	2 (not very)	3 (neutral)	4 (very)	5 (extremely)	Average
Availability of alternatives (e.g., sole-source)	19	0	1	2	11	5	4.1
Supplier location (e.g., weather, disasters)	21	1	0	5	8	3	3.7
Transportation disruptions	20	1	1	4	8	4	3.7
Geopolitical issues (e.g., war, IP treatment, sanctions)	19	1	1	5	7	5	3.7
Work stoppages (e.g., protests, riots)	21	2	3	5	5	2	3.1
Partnerships and reputational risk	20	0	4	4	6	4	3.6
Financial stability	20	0	1	3	11	3	3.9
ESG and ethical considerations	20	2	1	5	6	4	3.5
Raw material availability	21	1	0	3	5	8	4.1

Third-Party Risk Management: Component and Service "Health"

Category	Blank	1 (not at all)	2 (not very)	3 (neutral)	4 (very)	5 (extremely)	Average
Hygiene (e.g., security, quality)	19	1	0	2	8	8	4.2
Business continuity management (e.g., natural disasters, pandemics, geopolitical conflicts, etc.)	20	0	2	2	7	7	4.1
Asset creation	20	0	2	5	9	2	3.6
Asset integration	20	0	2	5	8	3	3.7
Labor availability	20	0	3	6	7	2	3.4

Special Topics in Supply Chain Business Continuity

Category	Blank	1 (not at all)	2 (not very)	3 (neutral)	4 (very)	5 (extremely)	Average
Distribution – Storage	19	1	4	4	6	4	3.4
Distribution – Transportation	19	1	4	5	5	4	3.4
Cloud service provider data storage	19	0	2	3	8	6	3.9
Cloud service provider subcontractors	19	0	2	4	8	5	3.8
Software Bill of Materials	19	0	2	2	9	6	4.0
Product attestations	19	0	3	4	4	8	3.9
Tooling and testing	19	0	3	6	6	4	3.6
Expansion and growth (manufacturing, data centers, etc.)	19	0	1	7	8	3	3.7
Expansion and growth (hiring and personnel)	19	0	3	6	10	0	3.4
Disaster recovery considerations	19	0	2	3	9	5	3.9

Cyber Supply Chain Security Results

24-29 respondents

Open Source and Third-Party Software

Category	Blank	1 (not at all)	2 (not very)	3 (neutral)	4 (very)	5 (extremely)	Average
Open source software integrity	9	1	1	4	10	13	4.1
Open source software provenance	9	1	2	5	9	12	4.0
Open source software ongoing support (e.g., maintenance)	9	1	1	6	15	6	3.8
Third-party software integrity	9	0	1	3	10	15	4.3
Third-party software provenance	9	0	3	1	14	11	4.1
Third-party software ongoing support (e.g., maintenance)	10	0	1	3	15	9	4.1

Cyber Vulnerabilities: Acquired Products

Category	Blank	1 (not at all)	2 (not very)	3 (neutral)	4 (very)	5 (extremely)	Average
Lack of regulatory/legal framework for responsibility	9	0	3	6	10	10	3.9
Built-in security requirements	9	0	1	5	12	11	4.1
Insufficient privileges for operation	10	0	3	8	10	7	3.8
Testing considerations	10	0	1	7	13	7	3.9
Integrity of tools (e.g., licensing, cloning, update/version & patching)	10	0	1	2	17	8	4.1
Malware and malicious code testing	9	0	1	4	6	18	4.4

Cyber Vulnerabilities: Produced Products

Category	Blank	1 (not at all)	2 (not very)	3 (neutral)	4 (very)	5 (extremely)	Average
Lack of regulatory/legal framework for responsibility	13	1	2	6	8	8	3.8
Built-in security requirements	12	1	0	4	12	9	4.1
Insufficient privileges for operation	12	1	3	8	10	4	3.5
Testing considerations	13	0	1	8	11	5	3.8
Integrity of tools (e.g., licensing, cloning, update/version & patching)	14	0	1	4	8	11	4.2
Malware and malicious code testing	14	0	0	3	8	13	4.4

Software Bill of Materials: Use Cases

Category	Blank	1 (not at all)	2 (not very)	3 (neutral)	4 (very)	5 (extremely)	Average
Resilience of incorporated components	11	1	2	3	11	10	4.0
Understanding components (vulnerabilities, maintenance/sustainment)	10	1	0	3	9	15	4.3
Passing risk/vulnerability to customer	11	0	2	0	6	17	4.4
Testing tied in	11	2	1	6	10	8	3.8
Attestation	10	1	1	4	9	13	4.1

Software Bill of Materials: Opportunities

Category	Blank	1 (not at all)	2 (not very)	3 (neutral)	4 (very)	5 (extremely)	Average
Automated construction	11	2	0	6	10	9	3.9
Higher fidelity in asset management	11	1	2	7	11	6	3.7
Concise information about supplied items	11	0	2	6	11	8	3.9

Software Bill of Materials: Types

Category	Blank	1 (not at all)	2 (not very)	3 (neutral)	4 (very)	5 (extremely)	Average
Deployment	11	0	0	5	10	12	4.3
Source code	11	1	2	5	11	8	3.9
Run-time	11	1	1	4	14	7	3.9

Special Topics in Cyber Supply Chain Security

Category	Blank	1 (not at all)	2 (not very)	3 (neutral)	4 (very)	5 (extremely)	Average
Stigma from cyber incident reporting – Within sector	11	2	2	5	15	3	3.6
Stigma from cyber incident reporting – From government	11	3	2	6	12	4	3.4
Sub-tier supply chain cybersecurity profile and compliance	12	1	0	5	13	7	4.0
Applicability of cybersecurity requirements and standards to supply chain	11	0	0	4	13	10	4.2

Next Steps

- Discuss areas of best practices and concerns **(ongoing)**
  - Identify common best practices
  - Consolidate into refined list applicable across various process implementations
  - Publish updated version of O-TTPF
- Determine integration of best practices into O-TTPS attributes and requirements
  - Consider implications for O-TTPS structure
  - Consider implications for O-TTPS Certification Program
- Develop content for review and publication

Questions

John Linford

J.Linford@opengroup.org

https://www.linkedin.com/in/johndouglaslinford/