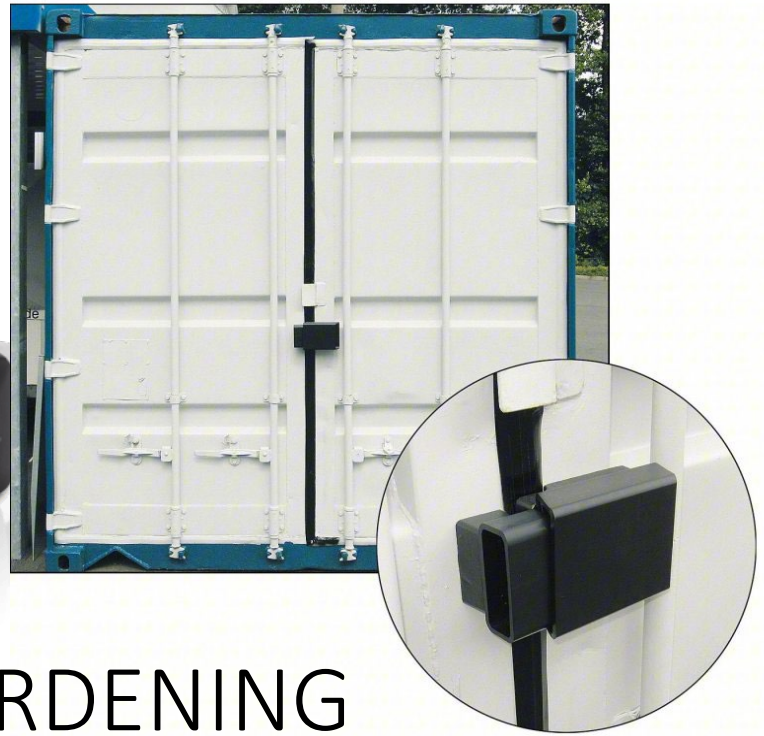
Physically Security: Hardening your Supply Chain & Physical Infrastructure

Compliance, Controls, & Common Sense

Thornton Tomasetti | HDR | ONE COMPANY *Many Solutions*®

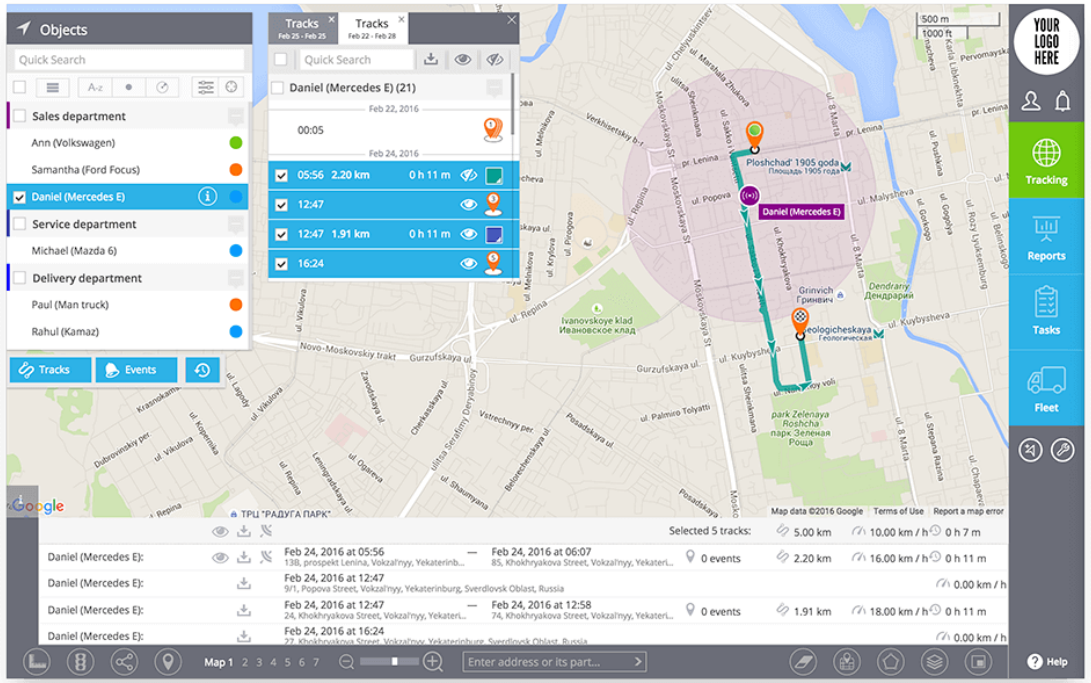
RISK MANAGEMENT – PHYSICAL SECURITY

- Risk Assessment – What are your threats and threat vectors?
- Vulnerability Assessment – Where are you weak?
- Mitigation – Strengthen against potential attacks and have a response plan before the attack.
- Re-Assessment – Continue to reassess



PHYSICAL HARDENING

TRACKING AND LOCATING



HDR | ONE COMPANY *Many Solutions*®

RISK MANAGEMENT – WHAT WILL IT COST ME?

- Recognition – Is There Really a Problem?
- Regulations – What Are You *Required* to Do?
- Threat Sources – Who/What Are they?
- Threat Source – Where Do They Come From?
- Threat Agent – Who/What Are They?
- Vulnerability – Where Are You Weak?
- Mitigation – What Can You DO About it?
- Risk Assessment – When Will You Be Done?

Is There Really A Problem?

- *"The Government Accountability Office found that of the 25 DOD major IT programs it reviewed, only 15 of those programs had department-approved cybersecurity strategy and just 10 had and submitted a system security plan for information and communications technology supply chain risk management."*

- *"…the department is in the process of enhancing Risk Management Framework guidance for the [supply chain risk management] family of controls, with tailoring guidance for components' implementation, "Tanya Skeen, the acting assistant secretary of defense for acquisition*

[The Pentagon should keep better tabs on IT cybersecurity, supply chain risks, GAO says - FCW]

By Lauren C. Williams, Senior Editor

[GAO 2022 Business Report to Congressional Committiees]

Is There Really A Problem?

- ISACA 2022 Global Research Report

- 1,300 Global Industry professionals surveyed around the globe with supply chain visibility and expertise.

Supply Chain Security Gaps: A 2022 Global Research Report, ISACA

Is There Really A Problem?

- Do you know……?
  - How critical is the application/product/service/software you receive from your vendors in your company being able to meet its deliverables?
  - What is the data that the product/products' software/products' service and/or application providing or storing for the customer on a regular basis?
  - Where are the vendor's headquarters?
  - What is the vendor's disaster recovery plan and notification of breach plans?
  - How many breaches or incidents of a cyber nature has the company been subject to in the last five years? Was there anything of concern?

What Are You ***Required*** to Do?

1. Cybersecurity Maturity Model Certification (CMMC)

2. DFARS Definition of Supply Chain Risk Change Number: DFARS Change 03/1/2023, Effective Date: 03/01/2023

3. DFARS Definition of Applicability Change Number: DFARS Change 03/1/2023, Effective Date: 03/01/2023

4. Buy American Act (BAA) & National Defense Authorization Act (NDAA) - Supply Chain Scrutiny & Government Contracting

1. *"It is designed to enforce protection of sensitive unclassified information that is shared by the Department with its contractors and subcontractors."*

2. *DFARS Regulation 252.239-7018: "The Contractor shall mitigate supply chain risk in the provision of supplies and services to the Government."*

3. *239.7302 Applicability: "Any contract action involving a contract for a covered system or a covered item of supply where such contract includes a requirement relating to supply chain risk."*

4. *"…companies found to have violated sourcing laws and regulations also may face suspension and debarment from government contracting, which disqualifies companies from bidding on and receiving new federal contracts and subcontracts."*

What Is A Threat Source? The Government's Definition

NIST SP 800-12 Rev. 1

Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

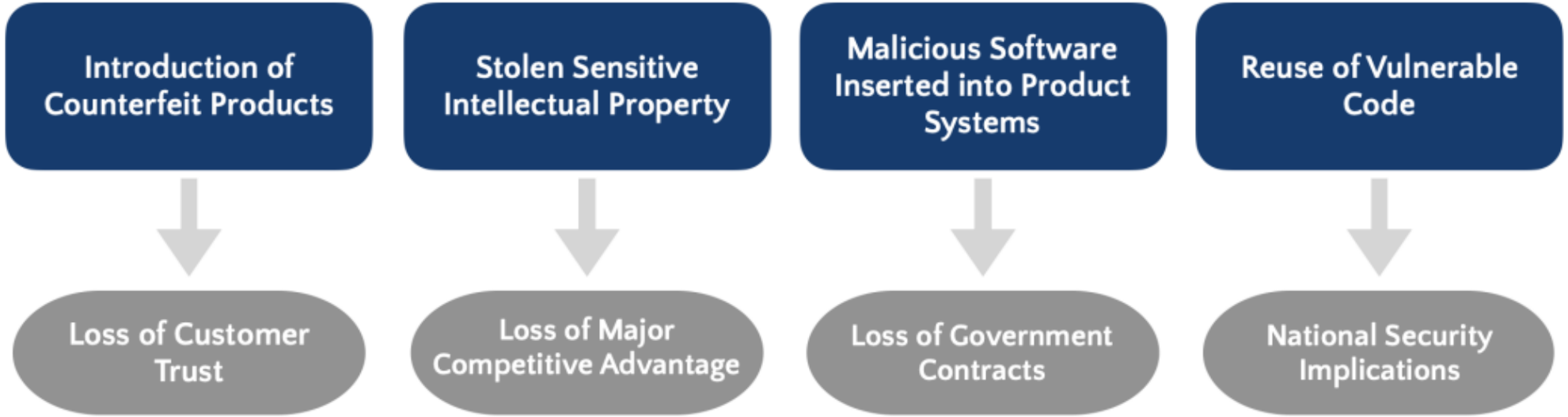
What Is A Threat Agent? The Government's Definition

NISTIR 7946

…"…An attacker's ability to successfully exploit a vulnerability based on how remote an attacker can be, from a networking perspective, to an information system."

Where Are You Weak?

Figure 1: NIST's Examples of the Impact Cybersecurity Risks Have on the Supply Chain

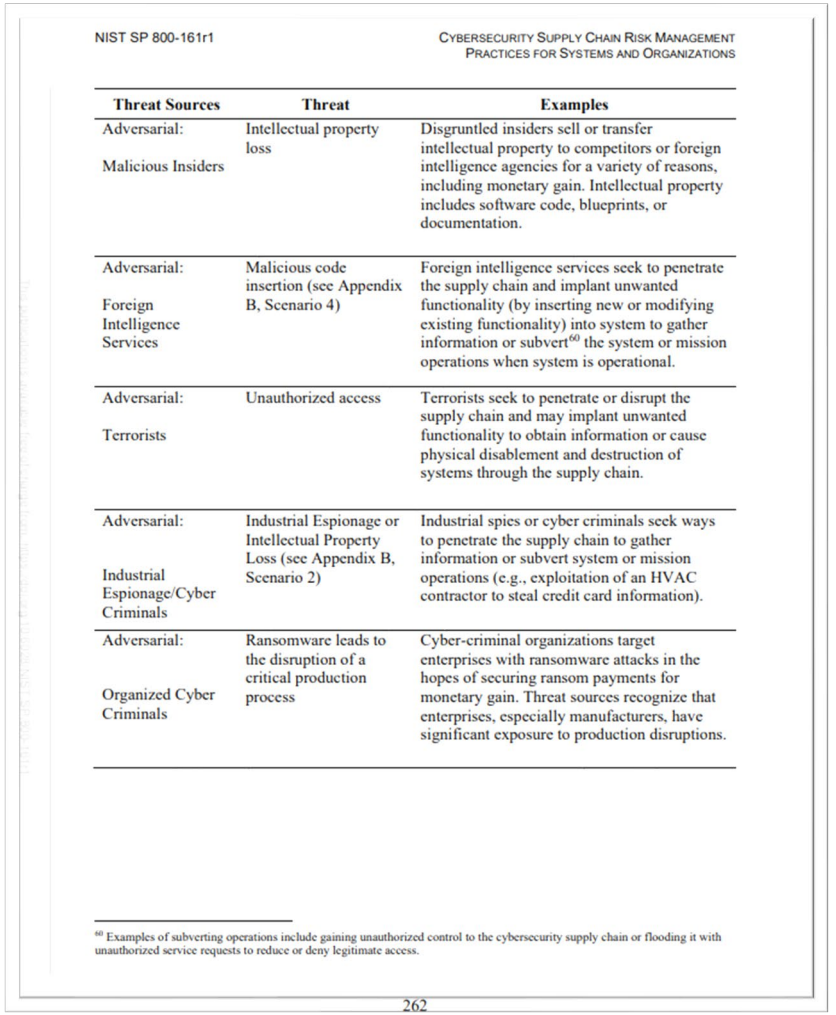


[Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
NIST SP 800-161r1]

Quick Reference Table

"Supply chain cybersecurity threats are similar to information security threats, such as disasters, attackers, or industrial spies."

NIST SP 800-161r1 CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT PRACTICES FOR SYSTEMS AND ORGANIZATIONS



NIST SP 800-161r1 CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT PRACTICES FOR SYSTEMS AND ORGANIZATIONS

Threat Sources	Threat	Examples
Adversarial: Malicious Insiders	Intellectual property loss	Disgruntled insiders sell or transfer intellectual property to competitors or foreign intelligence agencies for a variety of reasons, including monetary gain. Intellectual property includes software code, blueprints, or documentation.
Adversarial: Foreign Intelligence Services	Malicious code insertion (see Appendix B, Scenario 4)	Foreign intelligence services seek to penetrate the supply chain and implant unwanted functionality (by inserting new or modifying existing functionality) into system to gather information or subvert[60] the system or mission operations when system is operational.
Adversarial: Terrorists	Unauthorized access	Terrorists seek to penetrate or disrupt the supply chain and may implant unwanted functionality to obtain information or cause physical disablement and destruction of systems through the supply chain.
Adversarial: Industrial Espionage/Cyber Criminals	Industrial Espionage or Intellectual Property Loss (see Appendix B, Scenario 2)	Industrial spies or cyber criminals seek ways to penetrate the supply chain to gather information or subvert system or mission operations (e.g., exploitation of an HVAC contractor to steal credit card information).
Adversarial: Organized Cyber Criminals	Ransomware leads to the disruption of a critical production process	Cyber-criminal organizations target enterprises with ransomware attacks in the hopes of securing ransom payments for monetary gain. Threat sources recognize that enterprises, especially manufacturers, have significant exposure to production disruptions.

[60] Examples of subverting operations include gaining unauthorized control to the cybersecurity supply chain or flooding it with unauthorized service requests to reduce or deny legitimate access.

262

[Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations NIST SP 800-161r1]

What Can You *DO* About it?

- *"While there are cost-benefit trade-offs that must be acknowledged, the need to better secure supply chains is an imperative for both government and the private sector."*
  - 2018 SECURE Technology Act
  - Federal Acquisitions Supply Chain Security Act, Effective: 1 September 2020
  - NISTIR 8276 - Key Practices in Cyber Supply Chain Risk Management: Observations from Industry

Bottom Line Up Front: Its Just GOOD BUSINESS Practice!

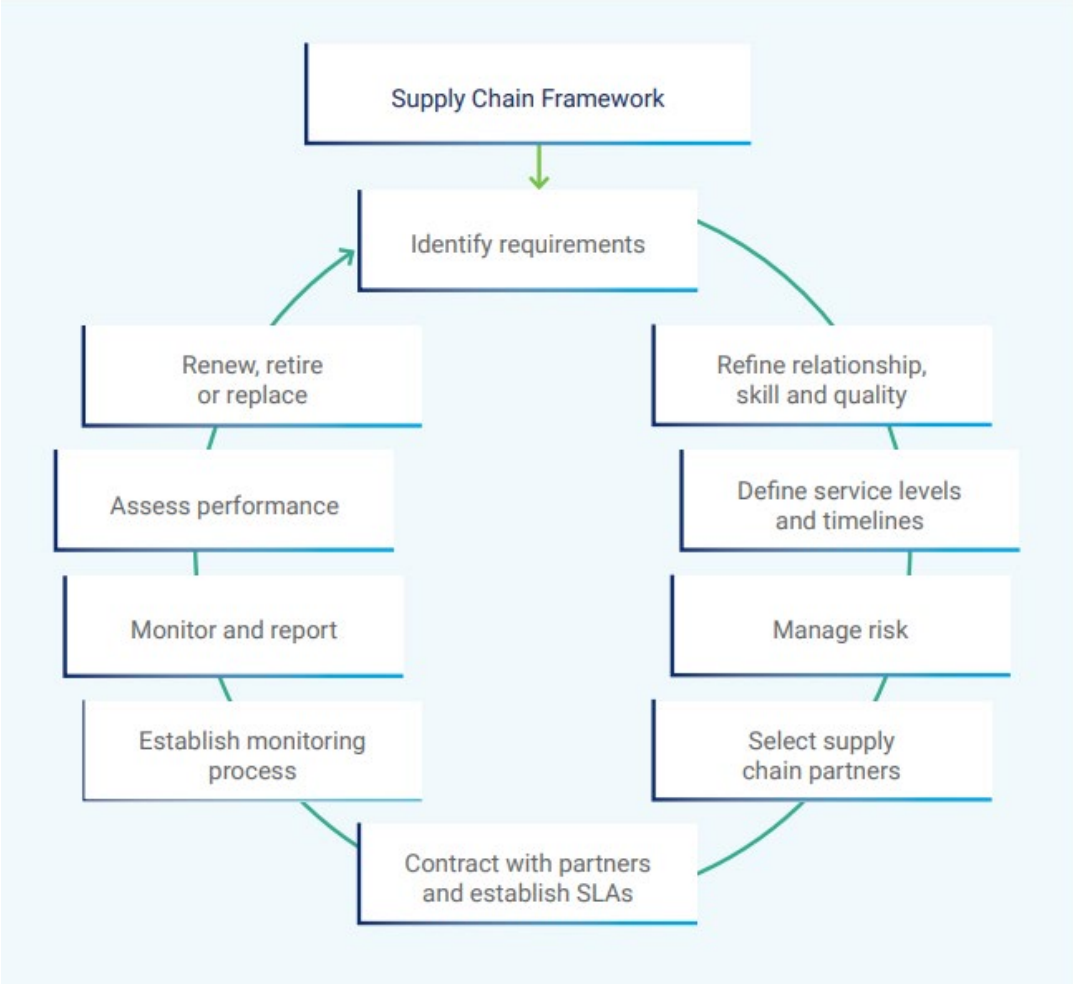
"(There is) a broad public and private sector consensus: C-SCRM capabilities are a critical and foundational component of any enterprise's risk posture."

What Can You *DO* About it?

- Educate Yourself and Your Company's Leadership
  1. U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency Interagency Security Committee, 2023 Edition
  2. 2023 Edition - Cost Analysis Template
  3. NIST Cybersecurity SCRM Fact Sheet
- Use Tools Already Out There
  1. OMB Nine Step Benefit-Cost Methodology
  2. US Army Cost Benefit Analysis Guide (CBA)
  3. ISACA Risk Resources

When Will You Be Done?

NEVER



Source: ISACA's "Supply Chain Resilience and Continuity" white paper.

BEST PRACTICES

- Practice Risk Management At All Levels
- Use Risk Assessments to Determine Threats and Vulnerabilities
- Develop Incident Response Plans to Ensure Business Continuity
- Evaluate Partners for Risk - Audits
- Ensure Compliance with All Partners – Consider Establishing SLA's
- Harden Both Physical and Logical Infrastructure
- Don't Trust Your Supply Chain – Limit Outside Access to Your Information

QUESTIONS

F. Charlene Watson
GICSP, CISSP, CISM |IAM/IAT L3, IASAE L2
HDR, Inc.
Charlene.Watson@hdrinc.com

Lewis W. Burns III
PSP, ISC2(CC)
Thornton Tomasetti
LBurns@thorntontomasetti.com