LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

HPH Cyber Supply Chain Risk Management (C-SCRM)

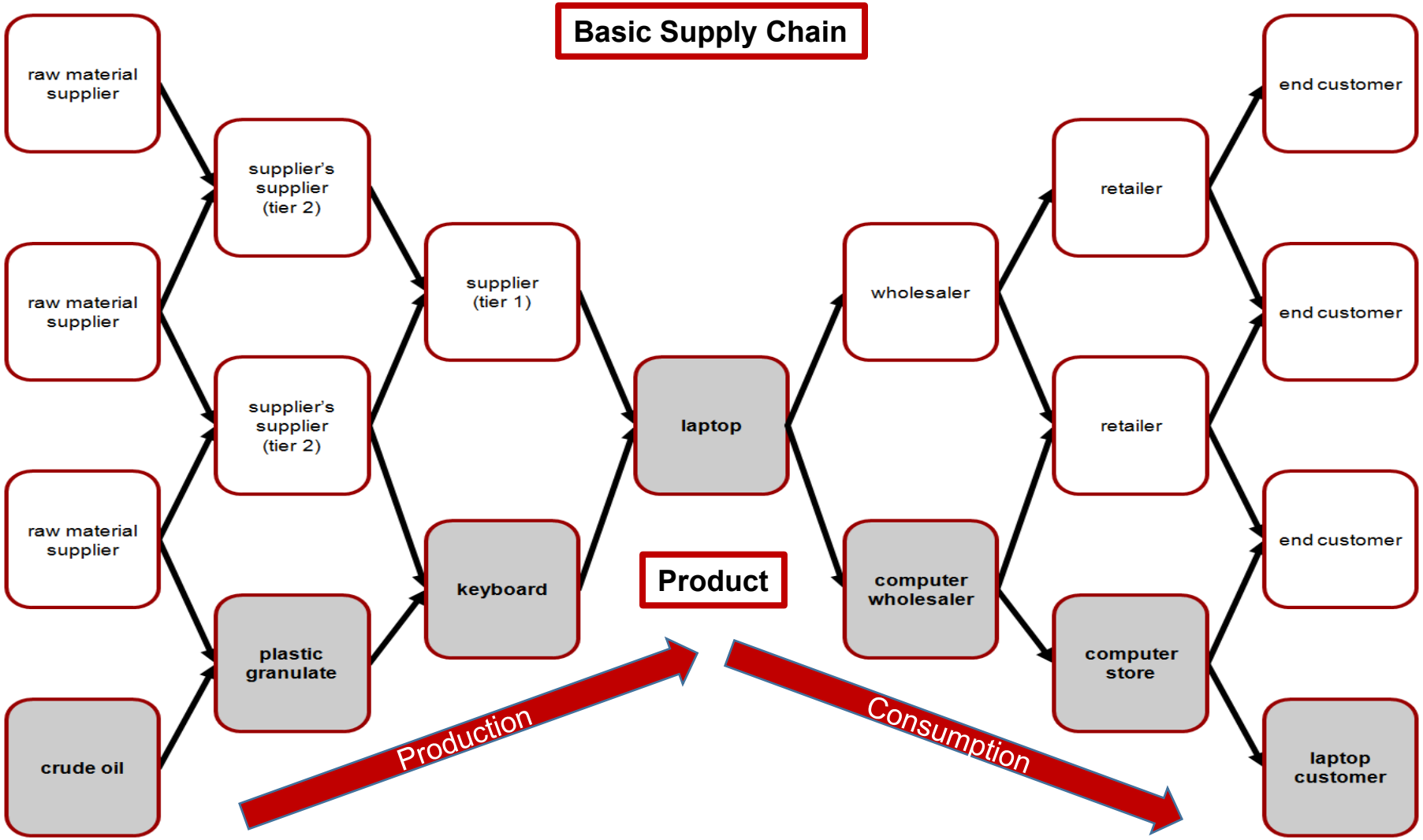
04/22/2021

TLP: WHITE, ID# ***202104221300***

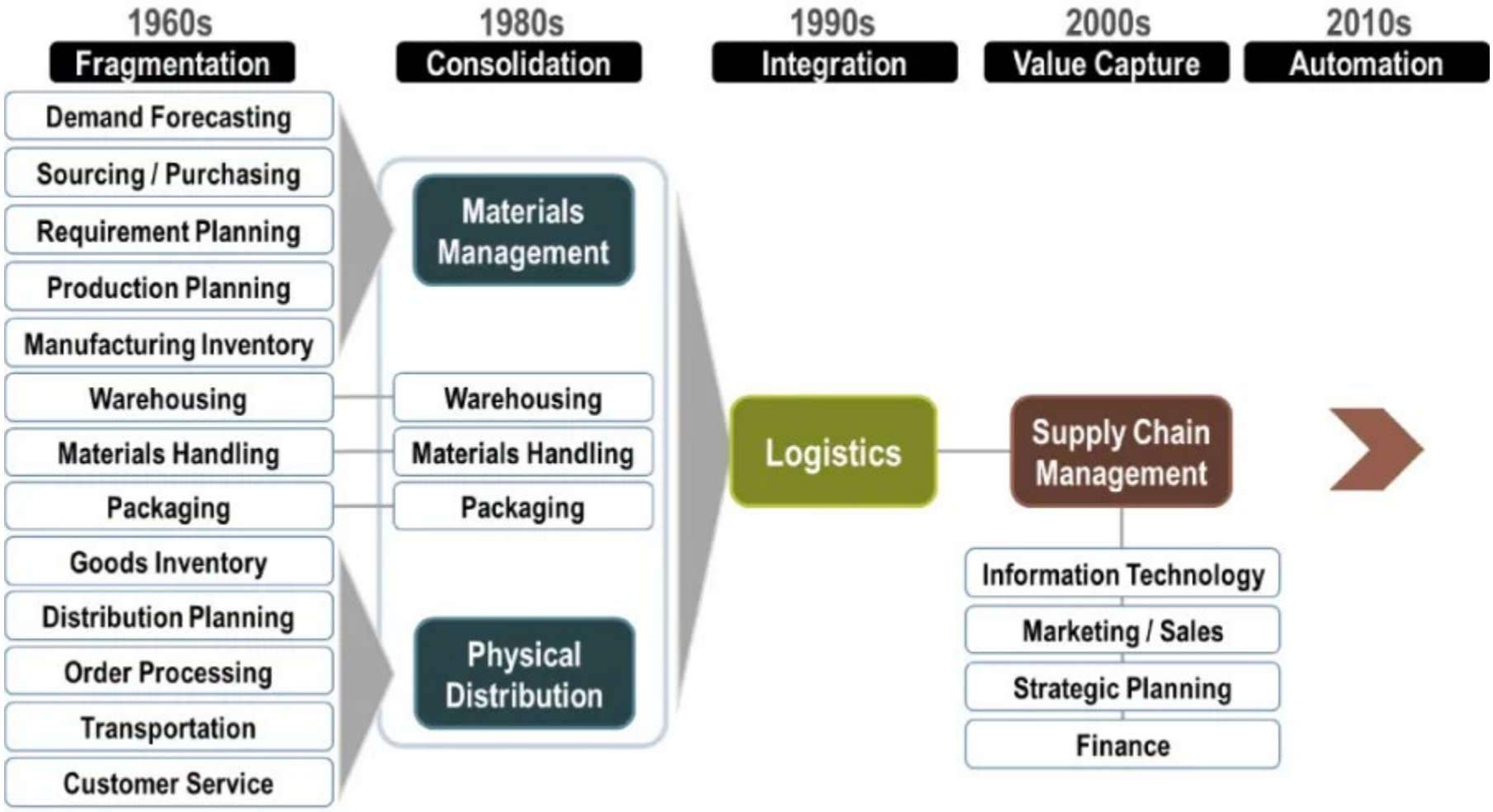
Agenda

- Introduction of the Supply Chain
- Supply Chain Attacks
- NIST Cyber Supply Chain Risk Management (C-SCRM) Project
- NIST Cybersecurity Framework (NSF) Updates
- NIST Case Studies in C-SCRM
- NISTIR 8276 Key Practices and Recommendations in C-SCRM
- HSCC Health Industry Cybersecurity SCRM Guide v2.0 (HIC-SCRiM)
- How to Conduct an SCRM Review
- Executive Orders
- Conclusion
- References
- Questions

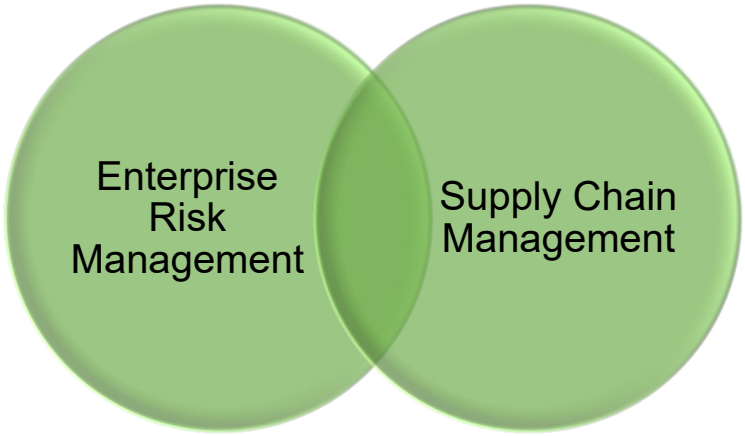
What is the Supply Chain?



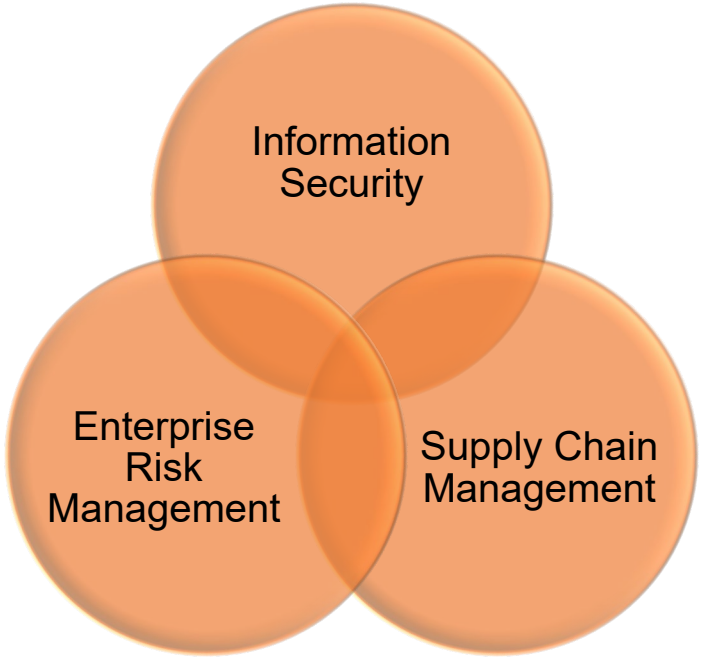
Evolution of the Supply Chain



The Birth of Cyber Supply Chain Risk Management

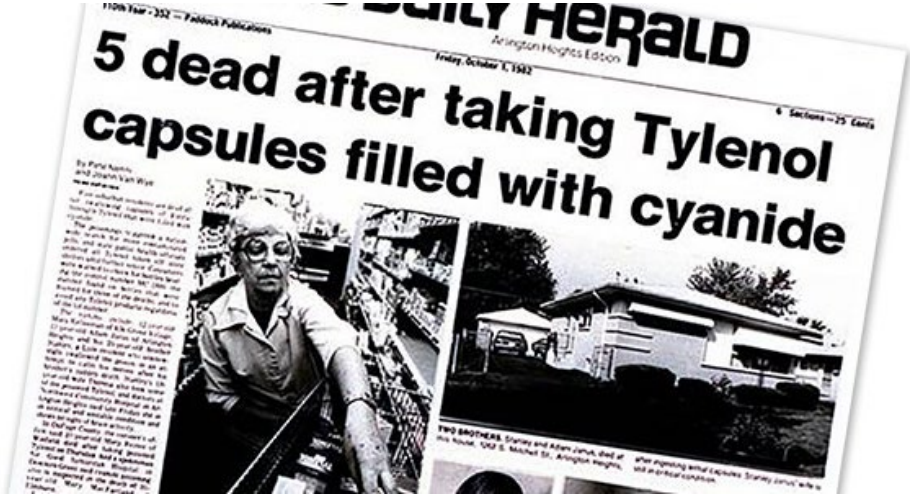


Supply Chain Risk Management



Cyber Supply Chain Risk Management

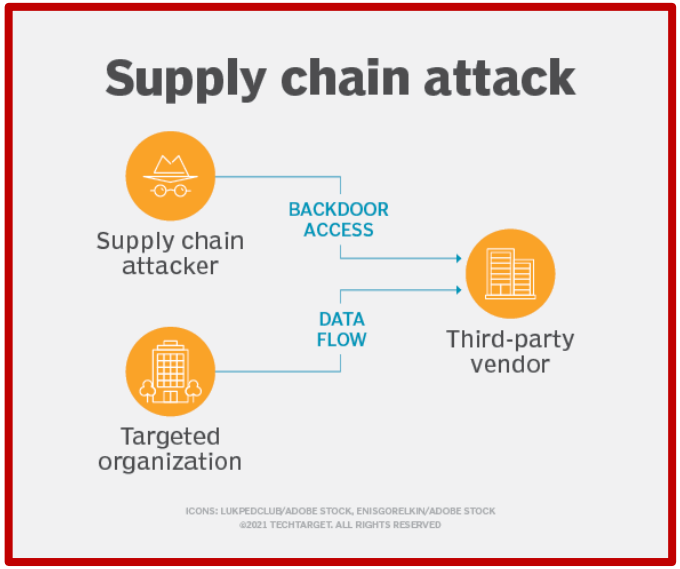
Supply Chain Attacks: Chicago Tylenol Murders

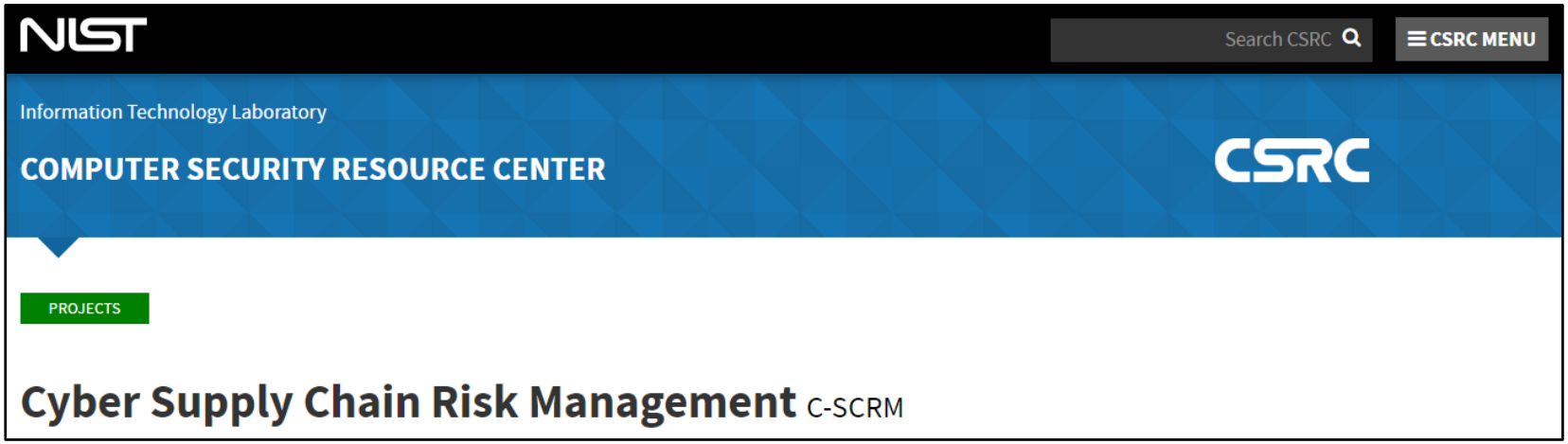


- September 1982
- Tylenol acetaminophen capsules laced with cyanide
- Seven people initially died – several others by copycats
- Police concluded culprit took bottles from stores, added cyanide, then returned bottles to store shelves
- No one was ever arrested
- Led to safety seals on products today

Supply Chain Attacks: Cyber

"Supply chain attacks are increasingly popular with attackers since they can access the information of larger organizations or multiple organizations through a single, third-party vendor."
– Identity Theft Resource Center





NIST develops:

- Standards, Guidelines, Tests, and Metrics

For the protection of:

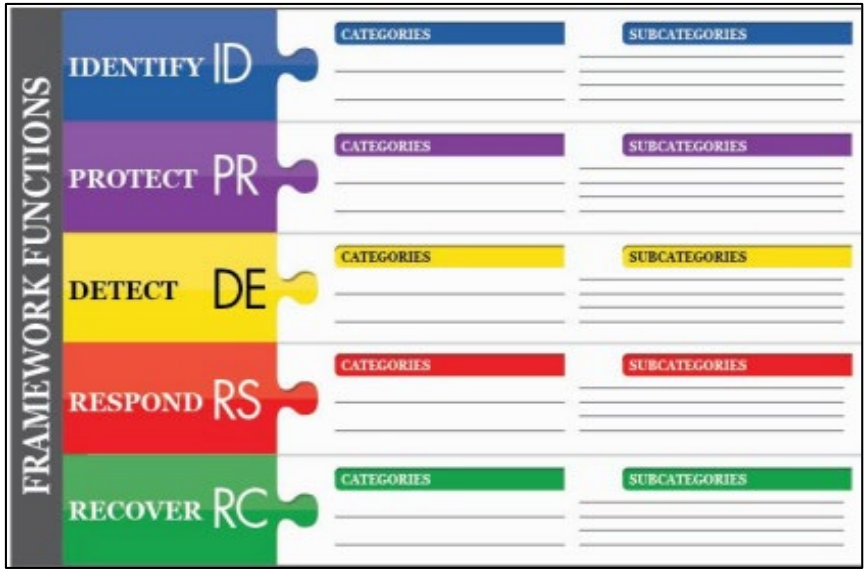
- Non-national security federal information and communications infrastructure
- Private sector and other government agencies

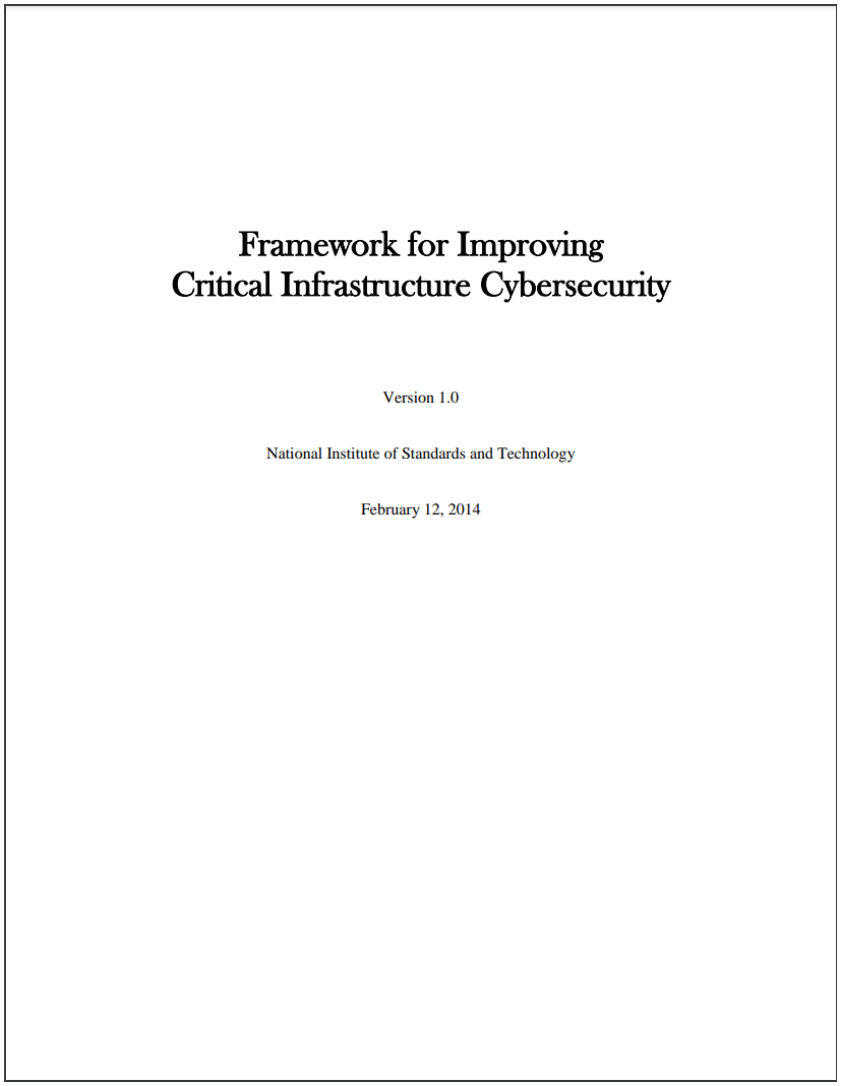
NIST C-SCRM focuses on:

- Foundational Practices
  - Best practices from InfoSec/SCM to create effective risk management
- Enterprise-Wide Practices
  - Fully engaging organization, business processes, and information systems
- Risk Management Practices
  - C-SCRM implemented as part of overall risk management program
- Critical Systems
  - HVAs identified

Cybersecurity Enhancement Act of 2014

"A prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks."





Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

Version 1.1, 2018

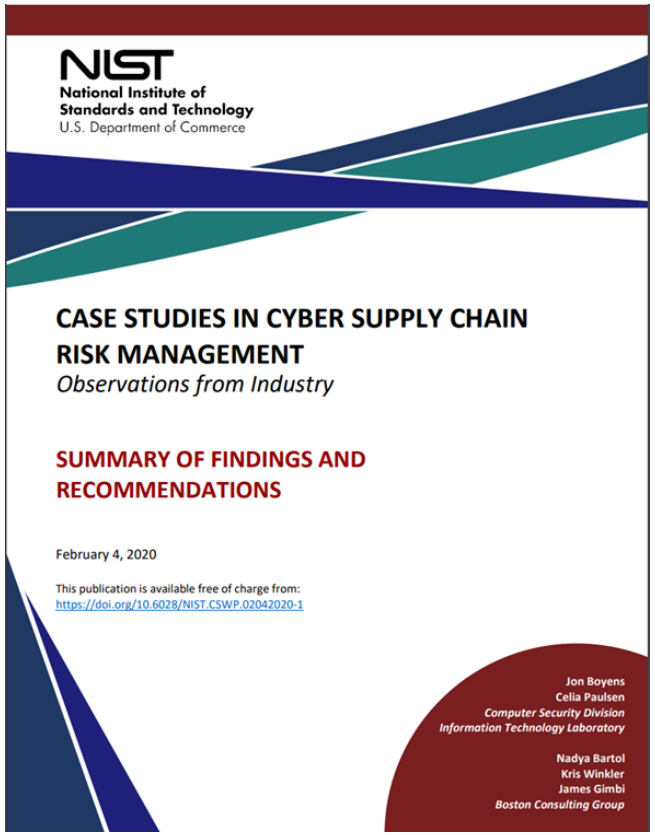
- Added SCRM category
  - 5 subcategories
- Expanded Sec. 3.3
  - Discuss C-SCRM
- Added Sec. 3.4
  - COTS risk

Function	Category	Subcategory
IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers

NIST Case Studies in C-SCRM

2019 case study series:

1. Mayo Clinic
2. Palo Alto Networks, Inc.
3. Seagate Technology PLC
4. Anonymous, Consumer Electronics Company
5. Anonymous, Consumer Goods Company
6. Anonymous, Renewable Energy Company



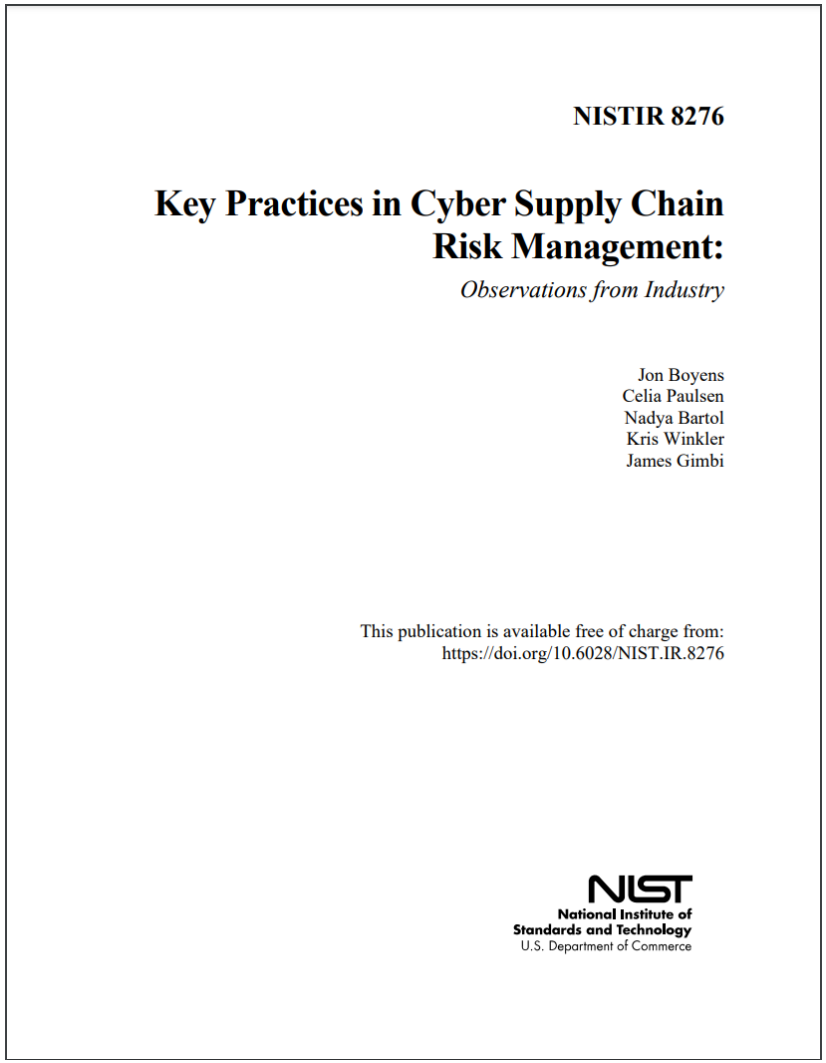
2015 case study series:

7. Boeing and Exostar
8. Cisco Systems
9. Deere & Company
10. DuPont de Nemours, Inc.
11. Exelon Corporation
12. FireEye
13. Fujitsu Ltd.
14. Great River Energy
15. Intel Corporation
16. Juniper Networks, Inc.
17. NetApp, Inc.
18. Northrop Grumman Corporation
19. Resilinc Corporation
20. Schweitzer Engineering Laboratories, Inc.
21. Smart Manufacturing Leadership Coalition
22. The Procter & Gamble Company
23. Anonymous, Communications Company
24. Anonymous, Utility

NISTIR 8276 Key Practices in C-SCRM

Key Practices:

1. Integrate C-SCRM Across the Organization
2. Establish a Formal C-SCRM Program
3. Know and Manage Critical Components and Suppliers
4. Understand the Organization's Supply Chain
5. Closely Collaborate with Key Suppliers
6. Include Key Suppliers in Resilience and Improvement Activities
7. Assess and Monitor Throughout the Supplier Relationship
8. Plan for the Full Life Cycle


NISTIR 8276

Key Practices in Cyber Supply Chain Risk Management:

Observations from Industry

Jon Boyens
Celia Paulsen
Nadya Bartol
Kris Winkler
James Gimbi

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8276

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8276 Key Practice 1: Integrate C-SCRM Across the Organization

Supply Chain Risk Councils Proactively:

- Review relevant risks and risk mitigation plans
- Set priorities
- Share best practices
- Pilot initiatives

Benefits of Councils:

- Shared risk decision-making
- Closer collaboration
- Better understanding of risks by Leadership

NISTIR 8276 Key Practice 2: Establish a Formal C-SCRM Program

Characteristics of formal C-SCRM Program:

- Increased Executive Board involvement for establishing C-SCRM as a top business priority
- Use of cross-functional teams
- Approved and banned supplier lists
- Use of software and hardware component inventory for third-party components
- Prioritization of suppliers
- Identification of alternative sources of critical components to ensure uninterrupted production

NISTIR 8276 Key Practice 3: Know and Manage Critical Components and Suppliers

Component and Supplier Criticality Criteria:

- Supplier revenue contribution
- Supplier processing of critical data or IP
- Volume of data or number of hosts
- Supplier access to network infrastructure
- Supplier potential attack vector to organization

Risks to supply chains include:

- Connectivity to suppliers
- Component sourcing
- Technology sharing
- Processes and People

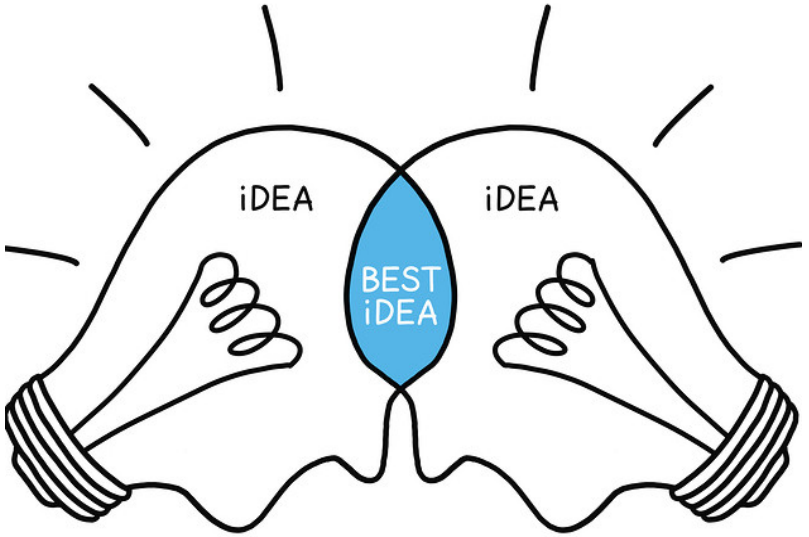
Best practice organizations have:

- Real-time visibility into production processes
- Insight into suppliers' personnel, who they outsource to, and who has access to their data

NISTIR 8276 Key Practice 5: Closely Collaborate with Key Supplier

Best practice organizations:

- Maintain close working relationships with their suppliers
- Mentor and coach suppliers on C-SCRM
- Invest in common solutions with suppliers
- Require the use of the same standards regarding cybersecurity risk and mitigation
- Use supplier questionnaires to identify opportunities for mentoring and training



NISTIR 8276 Key Practice 6: Include Key Suppliers in Resilience and Improvement Activities

Resilience and improvement activities can include:

- Rules and protocols for information sharing
- Joint development, review, and revision of IR, BC, and DR plans
- Communication protocols
- Response to cybersecurity incidents
- Coordinated restoration and recovery procedures
- Lessons learned processes
- Updates of coordinated response and recovery plans

NISTIR 8276 Key Practice 7: Assess and Monitor Throughout the Supplier Relationship

Monitor for risks:

- Security, privacy, quality, financial, and geopolitical

Ensure supplier is:

- Meeting cybersecurity and other SLA requirements
- Identifying changes in supplier status
- Mitigating risks according to schedule

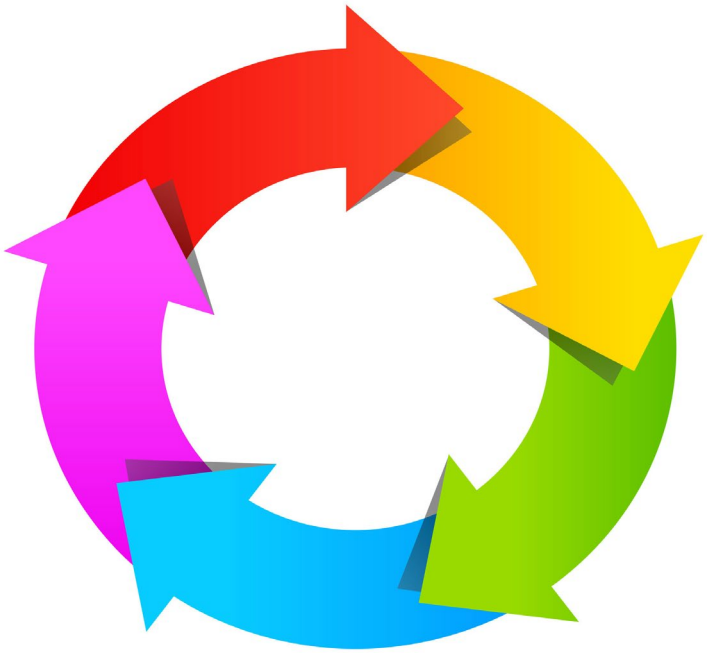
NISTIR 8276 Key Practice 8: Plan for the Full Life Cycle

Unexpected interruptions include:

- Discontinued hardware/software support
- Discontinued hardware production
- Supplier acquisition changing business direction

Mitigations to unexpected interruptions:

- Reserve quantities of critical components
- Relationships with approved resellers
- Bringing failing component manufacturers in-house



NISTIR 8276 Key Practices in C-SCRM

	Integrate C-SCRM Across the Organization	Establish a Formal C-SCRM Program	Know and Manage Critical Supplier	Understand Org. Supply Chain	Closely Collaborate with Key Suppliers	Include Key Suppliers in Resilience and Improvement Activities	Assess and Monitor Throughout Supplier Relationship	Plan for the Full Life Cycle
Number of Recommendations	13	20	16	12	15	8	4	4
Establish supply chain risk councils that include executives from across the organization (e.g., cyber, product security, procurement, legal, privacy, enterprise risk management, business units, etc.).	✓	✓						
Create explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, and physical security functions.	✓	✓						
Increase Executive Board involvement in C-SCRM through regular risk discussions and sharing of measures of performance.	✓	✓						
Integrate cybersecurity considerations into the system and product life cycle.	✓	✓						
Clearly define roles and responsibilities for the security aspects of specific supplier relationships.		✓			✓			
Use master requirements lists and SLAs to establish requirements with suppliers.		✓	✓					

NISTIR 8276 Key Practices in C-SCRM, II

	Integrate C-SCRM Across the Organization	Establish a Formal C-SCRM Program	Know and Manage Critical Supplier	Understand Org. Supply Chain	Closely Collaborate with Key Suppliers	Include Key Suppliers in Resilience and Improvement Activities	Assess and Monitor Throughout Supplier Relationship	Plan for the Full Life Cycle
Number of Recommendations	13	20	16	12	15	8	4	4
Propagate security requirements to suppliers' sub-suppliers.		✓	✓		✓			
Train key stakeholders in the organization and within the supplier's organization.		✓	✓		✓	✓		
Terminate supplier relationships with security in mind.	✓	✓	✓	✓				
Use the Criticality Analysis Process Model or BIA to determine supplier criticality.			✓					
Establish visibility into the suppliers' production processes (e.g., capture defect rates, causes of failure, and testing).			✓	✓	✓			
Know if the data and infrastructure are accessible to suppliers' sub-suppliers.			✓	✓	✓			

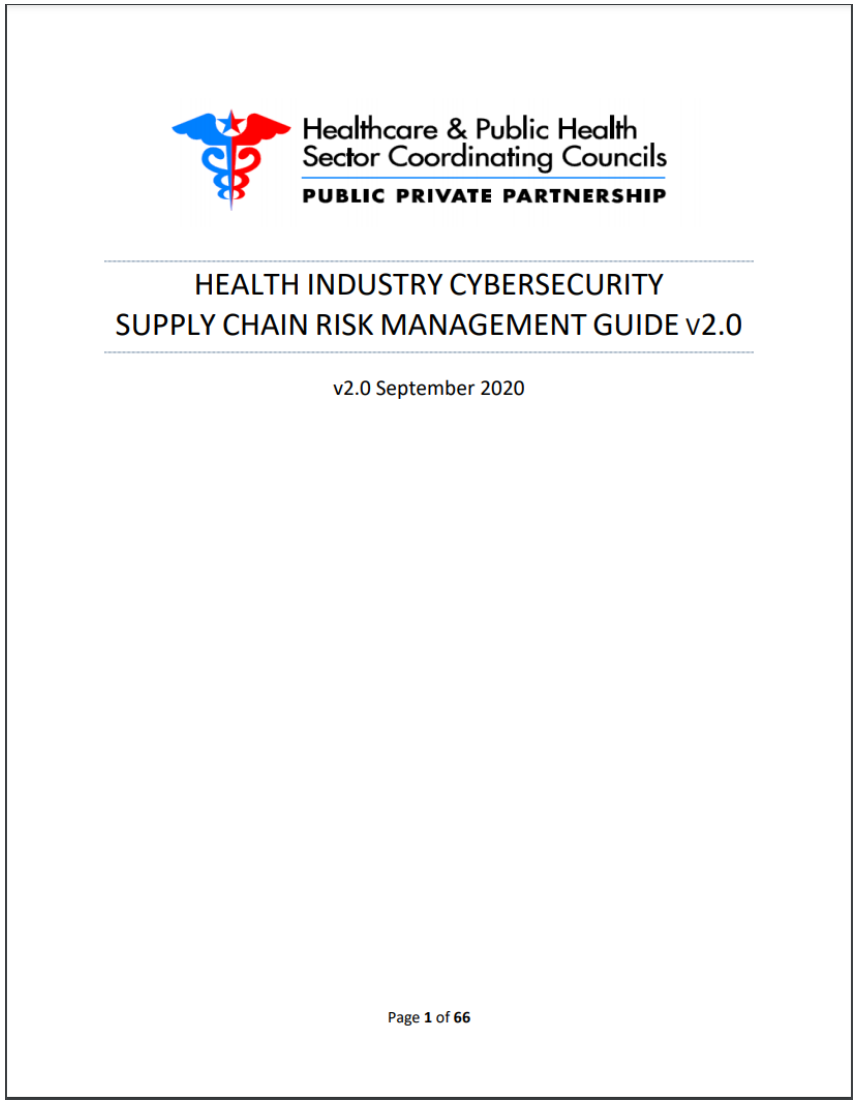
NISTIR 8276 Key Practices in C-SCRM, III

	Integrate C-SCRM Across the Organization	Establish a Formal C-SCRM Program	Know and Manage Critical Supplier	Understand Org. Supply Chain	Closely Collaborate with Key Suppliers	Include Key Suppliers in Resilience and Improvement Activities	Assess and Monitor Throughout Supplier Relationship	Plan for the Full Life Cycle
Number of Recommendations	13	20	16	12	15	8	4	4
Mentor and coach suppliers to improve their cybersecurity practices.					✓	✓		
Require the use of the same standards within both acquirer and supplier organizations.	✓	✓			✓			
Use acquirer assessment questionnaires to influence acquirer's cybersecurity requirements.		✓	✓		✓	✓		
Include key suppliers in incident response, business continuity, and disaster recovery plans and tests.	✓	✓	✓	✓	✓	✓		
Maintain a watchlist of suppliers who have had issues in the past and about which the acquirer should be cautious for future use (e.g., "Issue Suppliers"). Such suppliers should only be used after approval from the supply chain risk council.	✓	✓	✓	✓			✓	✓
Establish remediation acceptance criteria for the identified risks.	✓	✓	✓	✓	✓	✓	✓	✓

NISTIR 8276 Key Practices in C-SCRM, IV

	Integrate C-SCRM Across the Organization	Establish a Formal C-SCRM Program	Know and Manage Critical Supplier	Understand Org. Supply Chain	Closely Collaborate with Key Suppliers	Include Key Suppliers in Resilience and Improvement Activities	Assess and Monitor Throughout Supplier Relationship	Plan for the Full Life Cycle
Number of Recommendations	13	20	16	12	15	8	4	4
Establish cybersecurity requirements through a Security Exhibit, Security Schedule, or Security Addendum document. This document should be finalized in partnership with the risk council members and included in all master services agreements (MSAs) of all suppliers based on the risk associated with the supplier engagement.	✓	✓	✓	✓	✓		✓	✓
Establish protocols for vulnerability disclosure and incident notification.	✓	✓	✓	✓	✓	✓		
Establish protocols for communications with external stakeholders during incidents.	✓	✓	✓	✓	✓	✓		
Collaborate on lessons learned, and update joint plans based on lessons learned.	✓	✓	✓	✓	✓	✓		
Use third-party assessments, site visits, and formal certification to assess critical suppliers.		✓	✓	✓	✓		✓	
Have plans in place for supplied product obsolescence.		✓		✓				✓

HSCC Health Industry Cybersecurity SCRM Guide v2.0



Healthcare & Public Health Sector Coordinating Councils

PUBLIC PRIVATE PARTNERSHIP

HEALTH INDUSTRY CYBERSECURITY
SUPPLY CHAIN RISK MANAGEMENT GUIDE v2.0

v2.0 September 2020

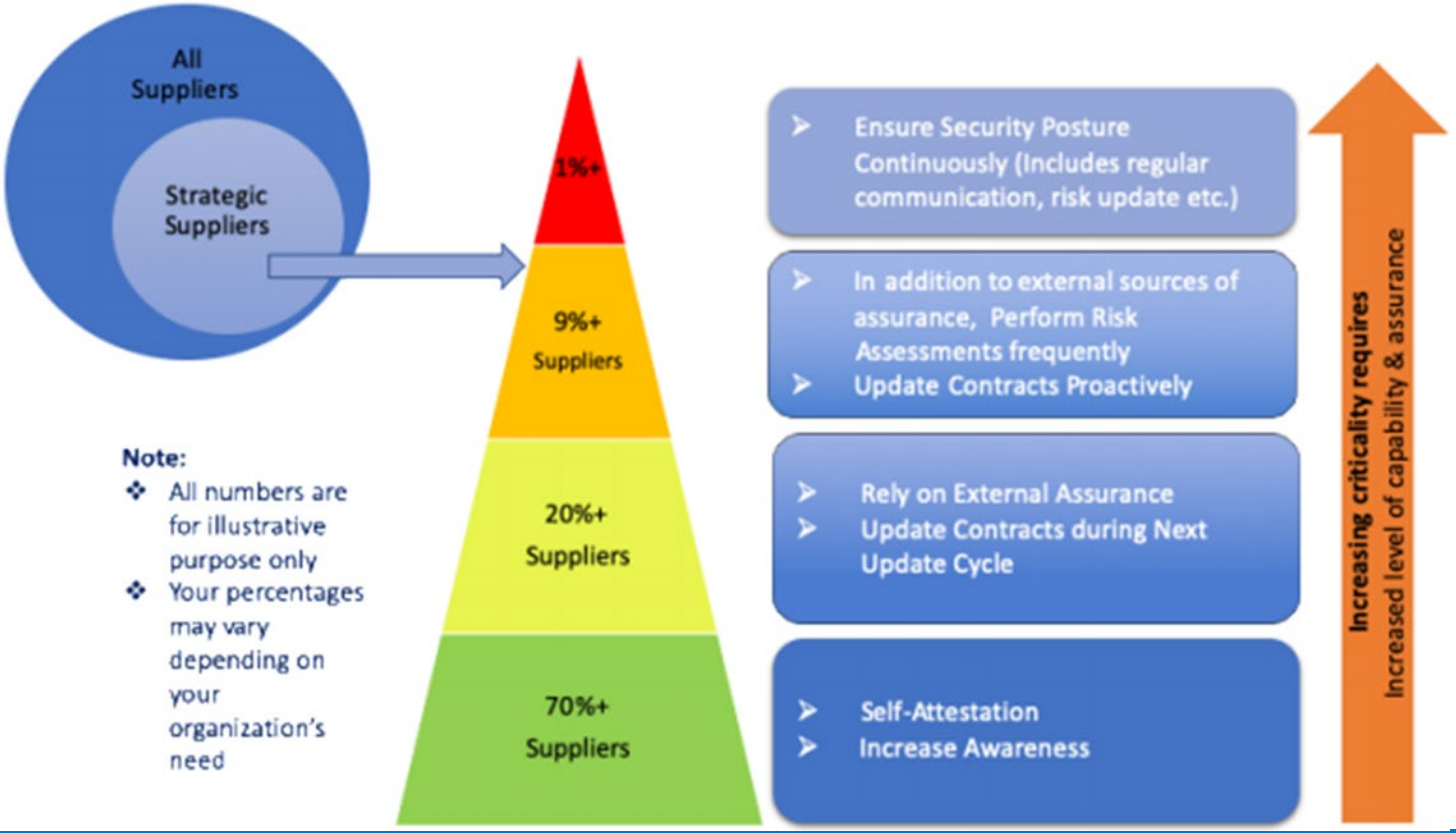
Page 1 of 66

ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders

1. Definition of Supplier Risk Areas
2. Definition of Roles and Responsibilities
3. Definition of Supplier Scope
4. Establishment of Policies and Procedures
5. Definition of a Supplier Risk Assessment Approach
6. Supplier Risk Management as Part of Business Operations

ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process

1. Define Organization's Supplier Risk Management Policy, and Establish Roles and Responsibilities
2. Identify Suppliers
3. Prioritize Suppliers
4. Assess Supplier Risk
5. Respond to Supplier Risk Assessment



ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan

Core (Mandatory) requirements

Cybersecurity Policy, Training and Awareness

1. Supplier shall have documented information security policies in place, refreshed annually, to ensure the confidentiality, integrity, and availability of Supplier and Company Information. These policies shall cover all business geographies and business functions of the Supplier, including their own sub-contractors/suppliers. These policies shall address the following core and supplemental requirements detailed in the agreed contract and shall ensure that enforcement mechanisms including training and awareness exist.

Asset and Change Management

2. Supplier shall maintain inventory of its information system assets, refreshed annually, that documents the identification, ownership, usage, location and configuration for each item. The Supplier shall ensure that changes to assets follow a documented change management procedure.

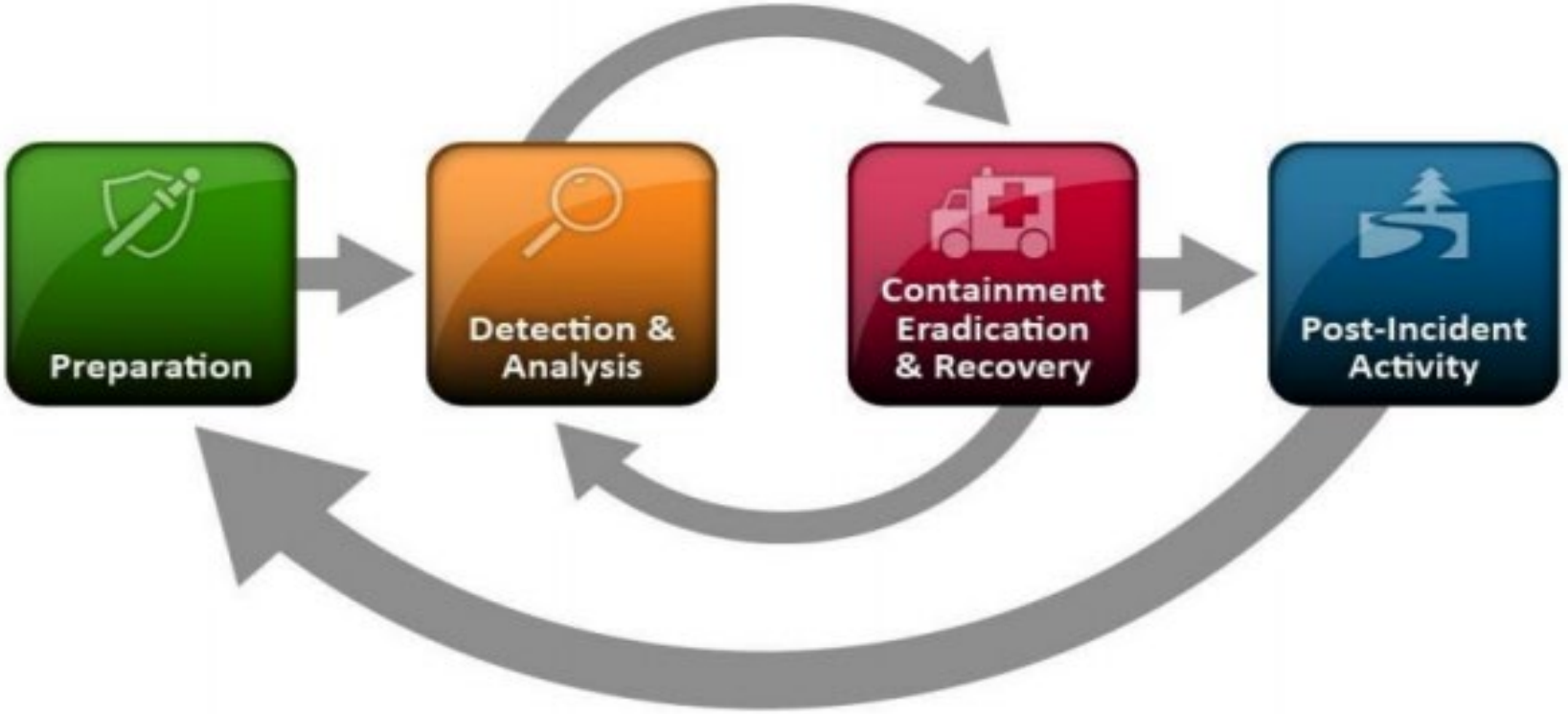
1. Guidance on the limitations of contracts in managing cybersecurity risk
2. Sample contractual boilerplate language for inclusion into contracts
3. Guidance on the Redlining Process
4. Guidance on how the buyer might obtain assurance that the terms of the contract are being fulfilled
5. Guidance on other contractual forms of risk transfer and avoidance (e.g. cyber insurance)

ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations

1. Defining the Audit and Verification Process
2. Identify Controls to be Verified and Method of Verification
3. Conducting Supplier Audits
4. Maintaining the Verification Process
5. Eliminating Gaps in Contractual Compliance

ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers

1. Creating the Plan
2. Testing the Plan
3. Post Testing Activity



BRIEFING ROOM

Executive Order on a Sustainable Public Health Supply Chain

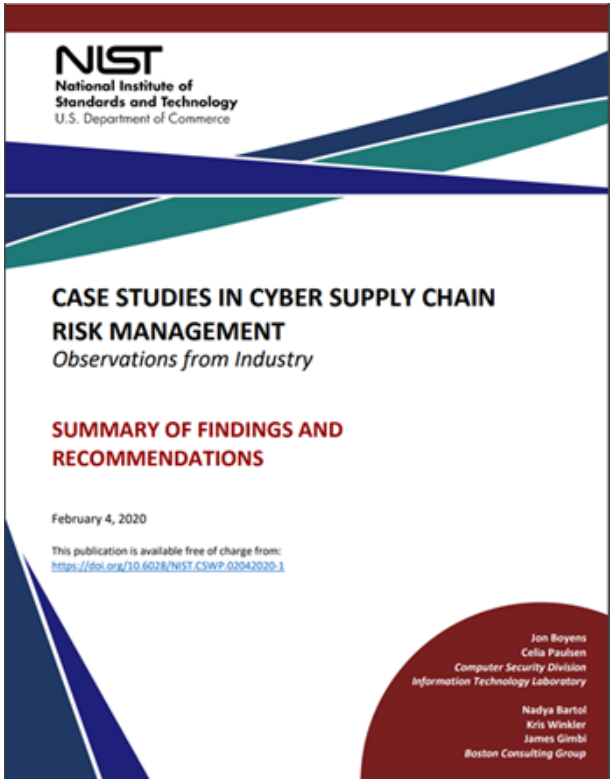
JANUARY 21, 2021 • PRESIDENTIAL ACTIONS

BRIEFING ROOM

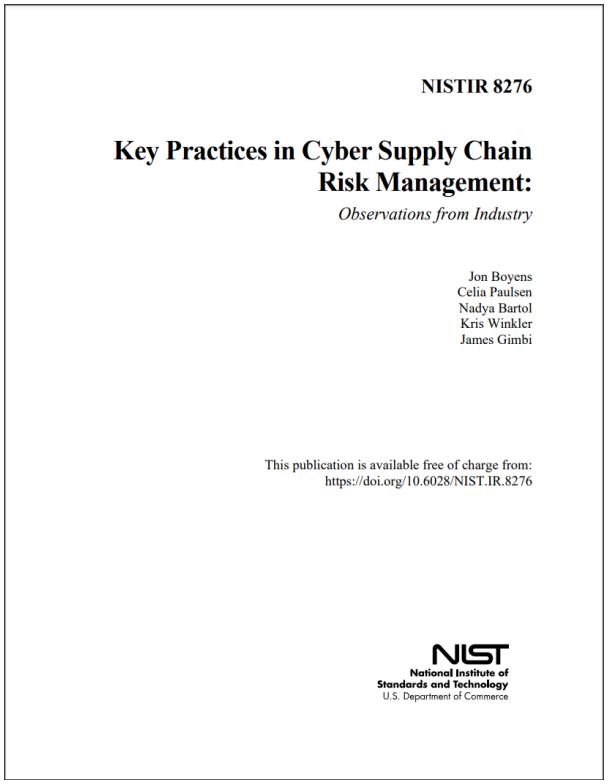
Executive Order on America's Supply Chains

FEBRUARY 24, 2021 • PRESIDENTIAL ACTIONS

Conclusion

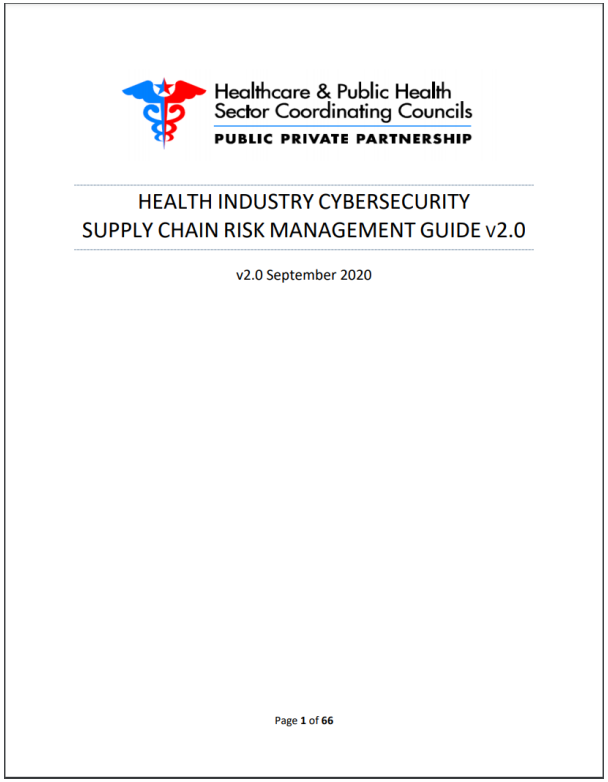


Industry Case Studies



8 Key Practices
24 Recommendations

Identify ID	Supply Chain Risk Management (ID.SC)	ID.SC-1
		ID.SC-2
		ID.SC-3
		ID.SC-4
		ID.SC-5



Reference Materials

Key References

- “Case Studies in Cyber Supply Chain Risk Management.” NIST. Accessed March 8, 2021. https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/key-practices
- “Case Studies in Cyber Supply Chain Risk Management. Observations from Industry,” NIST. Accessed March 8, 2021. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042020-1.pdf
- “Health Industry Cybersecurity Supply Chain Risk Management Guide v2.0,” Healthcare and Public Health Sector Coordinating Council. Accessed March 9, 2021. https://healthsectorcouncil.org/wp-content/uploads/2020/09/Health-Industry-Cybersecurity-Supply-Chain-Risk-Management-Guide-v2.pdf
- “NISTIR 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry,” NIST. Accessed March 8, 2021. https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf

References

- “Cyber Supply Chain Risk Management,” NIST. Accessed March 5, 2021. https://csrc.nist.gov/projects/cyber-supply-chain-risk-management
- “Executive Order on America’s Supply Chains,” White House. Accessed March 10, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/
- “Executive Order on a Sustainable Public Health Supply Chain,” White House. Accessed March 10, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/21/executive-order-a-sustainable-public-health-supply-chain/
- “Framework for Improving Critical Infrastructure Cybersecurity,” NIST. Accessed March 5, 2021. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- “HHS and HSCC Release Voluntary Cybersecurity Practices for the Health Industry,” Health Sector Council. Accessed April 13, 2021. https://healthsectorcouncil.org/hicp/
- “HSCC Shares Supply Chain Cybersecurity Risk Management Guidance,” Health IT Security. Accessed March 9, 2021. https://healthitsecurity.com/news/hscc-shares-supply-chain-cybersecurity-risk-management-guidance
- “More Than SolarWinds: Supply Chain Attacks Increasing,” Secure World Expo. Accessed March 13, 2021. https://www.secureworldexpo.com/industry-news/supply-chain-attacks-increasing
- “NIST Cybersecurity Framework: A cheat sheet for professionals,” Tech Republic. Accessed March 5, 2021. https://www.techrepublic.com/article/nist-cybersecurity-framework-the-smart-persons-guide/

References

- “SolarWinds attack explained: And why it was so hard to detect,” CSO Online. Accessed March 11, 2021. https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html
- “Supply chain attacks show why you should be wary of third-party providers,” CSO Online. Accessed March 11, 2021. https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html
- “Supply Chain,” Wikipedia. Accessed March 5, 2021. https://en.wikipedia.org/wiki/Supply_chain

Questions

Upcoming Briefs

- China Five-Year Plan (5/6)

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV, or call us Monday-Friday between 9am-5pm (EST), at **(202) 691-2110.**

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

HC3 Customer Feedback

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or call us Monday-Friday between 9am-5pm (EST), at (202) 691-2110.

Visit us at: www.HHS.Gov/HC3

Contact

www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV