FOUR PRACTICAL STEPS TO

Strengthen Your Cyber Supply Chain Risk Management

By Keith McCloskey, Vice President, National Security and Civilian, and
Charles D. Walker, Sr. Solutions Architect of Cyber Operations, National Security and Civilian

Introduction

Is your supply chain ready to defend against attacks from foreign entities and cyber adversaries? If not, the repercussions could be enormous.

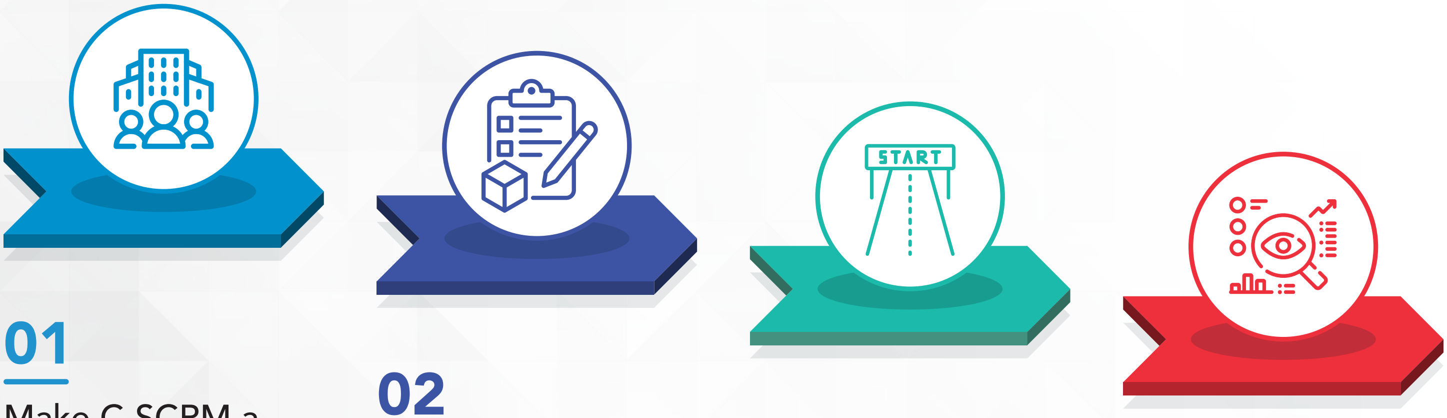
As demonstrated by events such as the **SolarWinds Orion** hack and the **Change Healthcare (CHC)** incident (the latter leading to an estimated $2.9 billion in losses), supply chains have become increasingly vulnerable to cyber threats in recent years, resulting in massive financial, operational, and reputational damage.

There are numerous reasons for growing cyber supply chain risk including:

- The rising depth and complexity of modern supply chains
- Mounting reliance on third-party vendors
- The increasing sophistication of cyber threats to exploit vendor entry points

In recent years, organizations have learned the hard way that securing their own networks is insufficient and that effective cyber supply chain risk management (C-SCRM) is needed to maintain oversight across their entire supplier ecosystem. Now is the time to consider potential attack surfaces and evaluate and prioritize your most critical assets, systems, and potential vulnerabilities as part of a comprehensive and integrated C-SCRM strategy.

Here are four actionable steps your organization should take to strengthen its C-SCRM protocols:



01

Make C-SCRM a shared enterprise-wide responsibility

02

Prioritize Vendor Visibility with a Software Bill of Materials (SBOM)

03

Consider C-SCRM from the Start

04

Move Beyond One-Time Assessments to Continuous Monitoring

01
Make C-SCRM a shared enterprise-wide responsibility

One of the most common mistakes organizations make is treating C-SCRM as a niche technical issue owned solely by cybersecurity teams. In reality, supply chain risk touches all aspects of an organization, making C-SCRM an enterprise-wide responsibility.

To break silos, your organization should establish clear ownership at the leadership level and encourage cross-functional input from relevant stakeholders (cybersecurity, procurement, legal, mission, etc.). At a practical level, you can improve cross-agency coordination by:

- Aligning C-SCRM activities with existing risk management and **cybersecurity** programs
- Ensuring acquisition and security teams communicate early in the procurement process
- Briefing senior leaders on supply chain risks in mission-focused terms

When C-SCRM becomes part of everyday decision-making, organizations are better positioned to address risk before it becomes a crisis.

02
Prioritize Vendor Visibility with a Software Bill of Materials (SBOM)

Organizations cannot manage supply chain risk if they do not know who their vendors/suppliers are or how critical they are to mission operations. While many enterprises work with hundreds or thousands of vendors, not all suppliers pose the same level of risk.

An effective approach is to start by building and maintaining a **Software Bill of Materials (SBOM)**, a basic inventory of suppliers, products, and services, and highlight those within the SBOM that support mission-critical systems or handle sensitive data. You could prioritize vendors/suppliers based on factors such as:

- The criticality of the system or service provided
- Access to federal data or networks
- Operational impact if the supplier were disrupted or compromised

This prioritization allows your organization to focus its limited resources in monitoring and scrutinizing high risk or high impact suppliers—where it matters most.

03
Consider C-SCRM from the Start

Many supply chain risks are introduced (often unintentionally) during procurement. When cybersecurity requirements are added late in the process, organizations may face higher costs, delays, or limited vendor options.

To improve C-SCRM outcomes, your organization should integrate supply chain considerations into acquisition planning from the very beginning. This can include:

- Clearly stating cybersecurity and supply chain risk expectations in RFPs
- Asking vendors about their security practices, subcontractors, and software dependencies
- Including contract language that supports transparency, reporting, and remediation
- Developing incident response and **continuity plans** (identifying alternate suppliers, mitigation strategies, clarifying roles, etc.) to fortify cyber resilience

When vendors understand expectations upfront, organizations gain better insight into risk and avoid surprises later in the lifecycle.

04
Move Beyond One-Time Assessments to Continuous Monitoring

Proper C-SCRM cannot be a one-time checklist completed during onboarding. In reality, supplier risk changes over time as vendors evolve, new vulnerabilities emerge, and threat actors adapt.

Organizations can strengthen C-SCRM by shifting toward ongoing monitoring and reassessment by:

- Periodically reviewing high priority suppliers for changes in risk posture
- Implementing **zero-trust architecture** across all environments
- Establishing processes for vendors to report security incidents or material changes
- Conducting exercises that include vendor compromise scenarios

Even simple, repeatable check ins can provide valuable early warning signs. Continuous monitoring helps move from reactive response to proactive risk management.

At a time when adversaries are increasingly targeting the weakest links in your supply chain, strengthening C-SCRM is not just a priority—it is essential to protecting your organization and securing public trust.

Review our 2025 Cybersecurity Report for information on C-SCRM and other important cyber trends.

From the boardroom to the battlefield, ECS empowers your mission, amplifies your impact, and drives lasting results with frontier technology solutions. Our highly skilled teams bring the best of innovation to urgent mission needs across the U.S. public sector, defense and intel, and commercial industries, with a focus on efficiency and impact. ECS maintains partnerships with leading AI, cloud, and cybersecurity technology providers and holds specialized certifications in their technologies.

V021026

ECStech.com