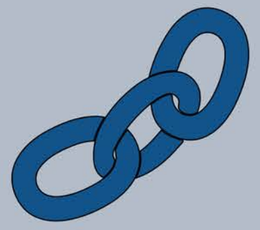
CyVidia

SUPPLY CHAIN RISK MANAGEMENT

MANAGING SUPPLIER & SUPPLY RISK

A Practical Roadmap for Building Supply Chain Security

SUPPLY CHAIN ATTACK OVERVIEW



What is it?

Attackers target the weakest link in the chain of systems

Compromising the trust with suppliers

How does it work?

Exploiting the trust and move through the connected chain

Attacks multiple targets at the same time

What is the impact?

Difficult to detect as trust is being violated

Results in brand damage, financial loss

Organizations consume and also deliver product and services. Most of them are right in the middle of supply chain concerns.

CyVidia

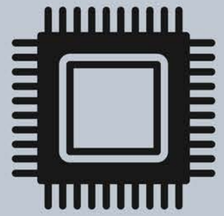
TYPES OF SUPPLY CHAIN ATTACKS

Targeting the weak links in the chain

SOFTWARE, INFRASTRUCTURE & DATA

Attacker compromise code components of software suppliers or poison training data for AI models

MoveIT, Kaseya, Solarwinds, Codecov



HARDWARE

Attackers target electronic & hardware manufacturers to change design, insert counterfeit

Toyota, Zyxel

HUMANS

Target vendor contact with sensitive information to gain entry before broader attack e.g. e.g ransomware attack

OKCPS, Discord, Doordash, AT&T

OPEN SOURCE

Attackers target open source code being use by developers in your organization

Log4j, NPM, Equifax

CyVidia

BUILDING CYBERSECURITY IN YOUR SUPPLY CHAIN

Cybersecurity Supply Chain Risk Management (C-SCRM) is a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures.

This brief guide is meant to get your supplier risk management program running in less than 2 Quarters. Let's get started.

01

GET YOUR TEAM INVOLVED

Include leadership, procurement, legal, security, engineering to create awareness and understand requirements

02

FOCUS ON THE FOUNDATIONAL PRACTICES

Start with items with red triangle on the next page before addressing the remaining items to mature your program

01

Manage Security & Compliance 2

- Establish SCRM *policies & procedures* including training
- Establish *supplier risk profile tiers*
- *Identify supplier, product security requirements mapped to customer requirements and frameworks*
- Integrate requirements in acquisition processes including open source software (OSS)

Know Assets & Supplier 3

- Identify, assess prioritize critica systems, proce *suppliers*
- Identify critical components an services that th organization pr and where it re including OSS
- Identify informa flows with critic suppliers

02

CyVidia

Supply Chain Risk Management (SCRM) Practices

CyVidia

Start with Foundational Practices ▲

1 Identify
The People

- ✓ Establish a PMO and integrate representatives from cybersecurity, IT, product dev., legal, logistics, audit, physical security, acquisition, marketing, and leadership
- ✓ Create information sharing, metrics, and program objectives
- ✓ Create program strategy & Implementation plan

2 Manage
Security & Compliance

- ✓ Establish SCRM policies & procedures including training
- ✓ ▲ Establish supplier risk profile tiers
- ✓ ▲ Identify supplier, product security requirements & controls mapped to customer requirements and frameworks
- ✓ ▲ Integrate requirements in acquisition processes including open source software (OSS)
- ✓ ▲ Establish incident response plan

3 Know
Assets & Suppliers

- ✓ Identify, assess and prioritize critical assets, systems, processes & *suppliers*
- ✓ ▲ Identify critical components / services including OSS and 3rd party software that the organization procures and where it resides
- ✓ Identify information flows with critical suppliers
- ✓ Establish contingency & DR plans for critical suppliers preferably in collaboration with them

4 Verify
Supplier & Supply Due Diligence

- ✓ ▲ Integrate requirements into suppliers' contractual language
- ✓ ▲ Identify specific methods, cadence & needed artifacts for assessing assurance and how they will be measured e.g. self-attestation, site visits, certifications, questionnaires etc.
- ✓ Validate supplier product for security vulnerabilities
- ✓ ▲ Conduct due diligence activities starting with critical suppliers

5 Monitor & Optimize

- ✓ ▲ Establish formal processes and intervals for continuous monitoring, remediation of issues & reassessment
- ✓ Continuously monitor acquired software and products vulnerabilities and exploitability
- ✓ Establish Center of Excellence to enhance and improve C-SCRM practices
- ✓ Establish collaboration and information sharing process with peers & critical suppliers to understand threats & improve practices

▲ Foundational Practices

SUPPLY CHAIN SECURITY FOUNDATIONS
6-month roadmap

PROGRAM OBJECTIVES
Create & Approve objectives with PMO driving cross-functional teams

Month One

REQUIREMENTS
Create supplier tiers and build requirements and controls for different tiers

Month Two

INVENTORY
Create complete inventory of all suppliers and what they provide. Focus on critical first

Month Four

VERIFY
Define & conduct due diligence process for starting with critical supplier tier
Define Contract SLAs

Month Five

MONITOR & OPTIMIZE
Define continuous monitoring process. Identify maturity areas e.g. software supply chain

Month Six

Crawl...Walk...Run
Identify your critical suppliers
Have leadership buy-in

CyVidia

MATURING BEYOND FOUNDATIONAL

Practices to focus once the foundations are established

Improving assessment process during procurement & acquistion

Use of additional methods e.g. SOC2, Ratings and Platforms

Collaboration with suppliers

Maintaining close relationships with critical suppliers to improve their practices. Organizations can play a role in raising the cybersecurity poverty line

Securing the Software & Data Supply Chain

Use of SBOMs, vulnerability exploitability, Open Source & 3rd party software due diligence, preventing data poisoning

Improving resilience

Improving the ability to recover from cyber disruptions to your suppliers e.g. building redundancies and increasing visibility using continuous monitoring

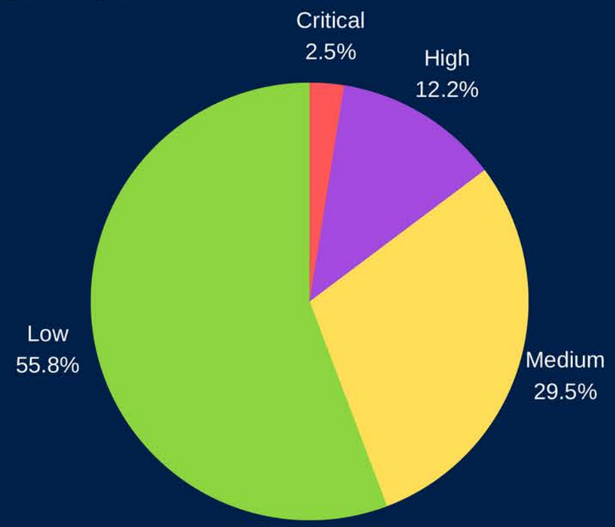
CyVidia

Tools & Techniques for your SCRM Program

Foundations

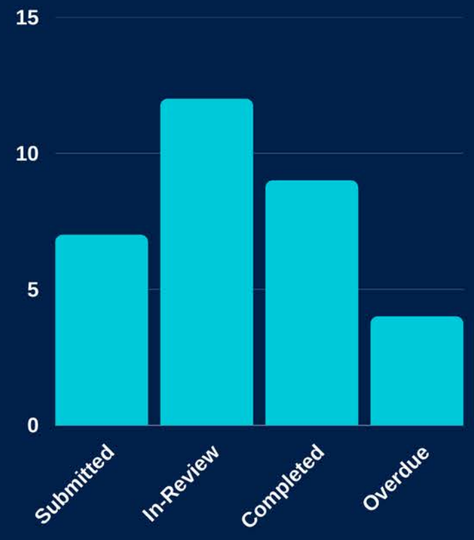
SCRM Dashboard

AGGREGATE SUPPLIER RISK SCORE



SUPPLIERS BY TIER

CRITICAL SUPPLIER LOCATIONS



ASSESSMENTS BY STATUS (Q2 23)

43

CRITICAL PRODUCTS

CRITICAL SUPPLIERS & ISSUES

Issues ▲ Suppliers ▲

Suppliers	Score
Sieno Manufactuing	C+
Acme Suppliers	C
TechInnovations	B-
NetCore	B-

NON COMPLIANT SUPPLIERS

CyVidia

Manage

SCRM Policy & Procedures

Table of Contents

1	**POLICY INTENT**	Purpose and Scope of SCRM policy including leadership intent e.g. enable enterprise risk owners to identify, assess, and mitigate supply chain risk to it's mission assets, functions, and associated services.
2	**POLICY STATEMENTS**	Mandatory high-level policy statements e.g. Assess and provide appropriate risk response to cybersecurity risks that arise from the acquisition and use of covered articles;
3	**ROLES & RESPONSIBILITIES**	Team responsible for the C-SCRM policies, as well as its key contributors including RACI
4	**IMPLEMENTATION PLAN**	Stand alone or specific to a system including types of information to be protected and potential impact of loss.
5	**REQUIREMENTS & CONTROLS (WHAT & HOW)**	Define SCRM requirements & controls e.g. supplier reviews, supplier access management, handling / disposal of PII or PHI data, SBOM, awareness training, off boarding

CyVidia

Know

Identify your Suppliers

Identifying **who** your suppliers are, **what** they provide and **how** they provide helps with:

- better insights into cyber security considerations that could be more easily enforced via contracts
- being more prepared to respond to supply chain related cyber incidents
- the ability to establish repeatable methods so you have confidence in suppliers' security practices, and help build long term partnerships
- easier compliance with legal, regulatory and or contractual responsibilities

STEPS

Build the Supplier, Supply and Services list

Using procurement systems or external tools build a full inventory of suppliers and sub contractors including relationships

Identify Critical Suppliers

Agree on a "Critical Supplier" definition and create tiers based on supplier criticality dependent on data processed, impact on revenue and customers

Create Data Maps

Document information flows with your critical suppliers including types of data,

Define Requirements & Update Controls

Based on the types of supplier, supply and the data being processed, update contract clauses due diligence process and assurance needs e.g. certifications

CyVidia

Verify

Supplier Contract Language Guidelines

Continuous Visibility

Periodic revalidation of supplier adherence to security requirements to ensure continual compliance

Continuous Communication

Processes and protocols for communication and the reporting of vulnerabilities, incidents, and other business disruptions, including acceptable deviations if the business disruption is deemed serious and baseline criteria to determine whether a disruption qualifies as serious

Secure Product and Software

The satisfaction of applicable security requirements in contracts and mechanisms as a qualifying condition for award and continued business

Responding to incidents

Terms and conditions that address the government, supplier, and other applicable third-party roles, responsibilities, and actions for responding to identified supply chain risks or risk incidents

CyVidia

Verify

Due Diligence Activities

Domain	Question #	Internal Question Details	Responses	Mitigation Ne
Internal Risk review	IR1	Do you consume more than 15% this supplier's sales of this product/service?	Yes No N/A	
Internal Risk review	IR2	Is product or service used enterprise wide in the organization?	Yes No N/A	
Internal Risk review	IR3	Is the product/service manufactured in a geographic location that is considered an area of geopolitical risk for your enterprise based on its primary area of operation (e.g., in the United States)?	Yes No N/A	
Internal Risk review	IR4	Is the product manufactured or developed in a country identified as a foreign adversary or country of special concern?	Yes No N/A	
Internal Risk review	IR5	Would switching to an alternative supplier for this product or service constitute significant cost or effort for your enterprise?		
Internal Risk review	IR6	Does your enterprise have an existing relationship with another supplier for this product/service?		
Internal Risk review	IR7	How confident is your enterprise that they will be able to obtain quality products/services regardless of major supply chain disruptions, both human and natural?		
Internal Risk review	IR8	Does your enterprise maintain a reserve of this product/service?		
Internal Risk review	IR9	Is the product/service fit for purpose? (i.e., capable of meeting objectives or service levels)?		

Internal Risk Assessment Questions

External Supplier Questionnaire

Mapped to NIST 800-53, 800-161 & 800-218

Domain	Question #	Questions	Responses	Clarifying questions	Sub domain
Secure Design & Engineering	3.1	Does your organization develop (or integrate) custom hardware or software offerings? List	Yes No N/A	3.1.1. List the custom software, hardware, system, or solution offering(s) provided by your organization.	
	3.2	Do you implement formal organizational roles and governanceresponsible for the implementation and oversight of Secure Engineering across the development or manufacturing process for product offerings?	Yes No N/A	3.2.1. If so, how are roles, responsibilities, and practices validated?	Product offering lifecycle management
	3.3	What security control framework (industry or customized) is used to define product offering security capabilities?	Yes No N/A	Please describe or 'N/A'	Product offering lifecycle management
	3.4	Does your organization document and communicate security control requirements for your hardware, software, or solution offering?	Yes No N/A	3.4.1. How are security requirements validated as part of the product offering development or manufacturing process?	Product offering lifecycle management
	3.5	How does your organization implement development andmanufacturing automation to enforce lifecycle processes and practices?	Yes No N/A		Product offering lifecycle management
	3.6	Does your organization protect all forms of code from unauthorized access and tampering, including patch updates?	Yes No N/A	How does your organization prevent unauthorized changes to code, both inadvertent and intentional, which could circumvent or negate the intended security characteristics of the software?	Protect IP
	3.7	Does your organization provide a mechanism for verifying software release integrity, including patch updates for your software product offering?	Yes No N/A		Protect IP
	3.8	How does your organization prevent malicious and/or counterfeit IP components within your product offering or solution?	Yes No N/A		Protect IP
	3.9	Does your organization manage the integrity of IP for its product offering?	Yes No	How does your organization archive assets associated with the product offering development or manufacturing process?	Protect IP

Contact us at info@cyvidia.com

CyVidia

CyVidia

Our services

Building trust in the supply chain

Cyber supply chain program build

Dashboards, policies, training, 3rd party assessment tools, scoring and incidence response plans

Secure Product Development

Product and Application security program assessment, risk score cards, SBOM implementation, training curriculum development

Contract & Regulatory Compliance

Monitor compliance & build actionable insights to ensure alignment with customer cybersecurity contract clauses and relevant regulatory guidance

Customer Due Diligence Support

Using AI and machine learning to answer due diligence questions from customers to speed up sales processes, provide more accurate information, and improve customer confidence.

info@cyvidia.com