What supply chain risks exist?

According to the National Institute of Standards and Technology (NIST), examples of supply chain risk include:

- Counterfeits and unauthorized production
- Tampering
- Theft
- Insertion of malicious software and hardware
- Poor manufacturing and development practices

What are some ramiFcations of attacks on the supply chain?

Supply chain attacks can lead to:

- Data loss
- Financial loss
- Compromise of product integrity or safety
- Brand and reputation damage
- Legal exposure
- Loss of life

What makes SCRM diMcult?

Suppliers are outside entities that oNer varying levels of transparency into their business policies and practices. Without visibility and industry standards, it's diMcult to assess the level of risk that suppliers may introduce into your organization.

What is C-SCRM?

Cyber SCRM (C-SCRM) addresses potential risks to the IT, OT, and communications technologies that are essential to your organization's mission. It even includes cybersecurity vendors and the products, software, and services that defend your organization against cyber attacks.

What SCRM best practices are available?

While there are many sources of best practices, the NIST makes many publications freely available.

What innovative C-SCRM approaches are there?

The U.S. Department of Defense (DoD) relies on hundreds of contractors and research institutions, which could introduce supply chain risk. Of particular concern is the security of sensitive information the department holds. Its new Cybersecurity Maturity Model Certification (CMMC) is an innovative program that aims to ensure its suppliers properly protect DoD data from cyber attacks.

Security

Security addresses the conFdentiality, integrity, and availability of the supply chain, its participants, and the data that travels across it.

Learn about Cisco Secure ›

Integrity

Integrity aims to ensure that products are genuine, unaltered, and will perform as intended without unwanted functionality. Visit our

Trust Center ›

Resilience

Resilience is focused on ensuring that supply chains function properly under pressure, stress, and even failure.

Reimagine business resilience ›

Quality

Quality is aimed at reducing vulnerabilities that can be exploited, cause failures, or limit the intended function of products and services. See our approach to quality ›