THREATS
Supply chain threats target organizations from the following vectors:

Adversarial Ownership
Suppliers may be owned, controlled, or influenced by an adversarial nation-state actor. Will this expose your organization's assets?

Cyber
Cyber threat actors may target your suppliers to gain unauthorized access to your IT assets and systems. What is your supplier's cyber posture? Does it match yours?

Geographical
Global suppliers must abide by the laws of the country in which they operate. Are those countries able to access your assets due to your supplier's global footprint?

Insider
Personnel security checks are in place to protect your employees and assets. But what controls are in place for a supplier's employees?

Physical
Facility security protocols stop unauthorized access, destruction, or damage to employees and assets. How does your supplier mitigate these same physical vulnerabilities?

Technology
Employees and critical assets operate on IT. Could outdated technology expose your organization or your suppliers' organizations to vulnerabilities that adversaries could exploit?

To address these threats, Supply Chain Risk Management (SCRM) Programs need an A.C.E.: Acquisition Security, Cyber Security, and Enterprise Security principles and best practices.

ADVERSARIES
• Nation-state actors
• Competitors (especially industry owned or influenced by nation-state actors)
• Malicious insiders
• Criminal organizations
• Hacktivists

If an adversary leverages an opportunity within the supply chain lifecycle, impacts to your organization could include:
• Delayed or degraded production
• Lost intellectual property or competitive business advantage
• Compromised privacy or security
• Disruption of services

COMMON METHODS OF SUPPLY CHAIN ATTACKS
• Cyber compromise
• Theft/interdiction
• Break/fix subversion
• Reroute
• Malicious component insertion
• Repair part compromise
• Trojan insertion/design to fail
• Fraud/counterfeit

PRODUCT OR SERVICE LIFECYCLE

ADVERSARIES
• Nation-state actors
• Competitors (especially industry owned or influenced by nation-state actors)
• Malicious insiders
• Criminal organizations
• Hacktivists

METHODS AND POTENTIAL IMPACTS OF SUPPLY CHAIN ATTACKS

SECURING YOUR ECOSYSTEM

CUSTOMER OR BUSINESS PARTNER OPERATIONS
THIRD PARTY RISK
If a third-party customer or business partner is compromised, the product or service they are providing may:
• Compromise information systems
• Expose sensitive national security information
• Disrupt or degrade operations
• Result in legal or reputational impacts

#SCRM is the A.C.E.
Acquisition Security | Cyber Security | Enterprise Security