interos

# Supply Network Security Challenges for the CISO

## Evolution of Supply Chain Attacks

Supply chain attacks are hard to define. There are multiple opinions in the cybersecurity community as to what constitutes a supply chain originating attack.

- **The First One - Heartbleed**
  The first attack commonly attributed to the supply chain was the OpenSSL TLS software bug uncovered in April 2014. OpenSSL was a widely used open-source software library that provided cryptographic functionality in many commercial software applications. It is estimated to have affected almost 30% of all Internet web servers and dozens of common vendors like Cisco. A patch resolved the problem, but criminal organizations exploited this bug to steal financial information.

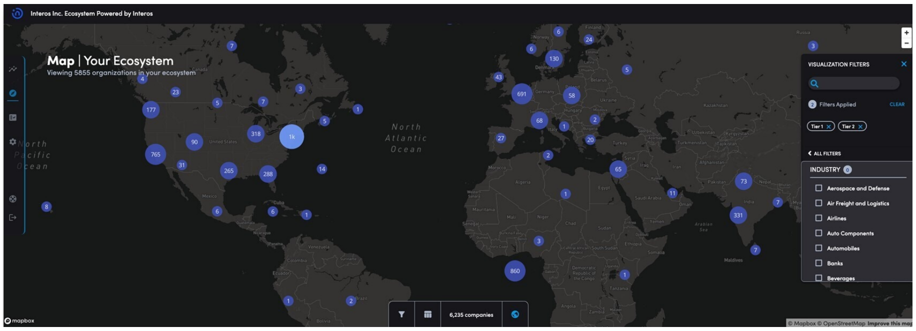
- **The Big One - SolarWinds**
  SolarWinds is a widely deployed infrastructure management and monitoring solution. In 2020 criminals were able to insert malicious code libraries at SolarWinds, which were pushed as an update to existing customers. The hack was fixed with a patch, but since SolarWinds has access to the entire network, a significant amount of intellectual property (IP) was stolen. Given the amount of time, effort, and expertise needed to accomplish this attack, experts believe it to be state-sponsored.

- **Rise of Ransomware - Kaseya**
  Kaseya is a commonly used patching service for updating older operating systems. It was compromised like SolarWinds, but this time ransomware was widely deployed. Victims paid the criminals to unlock their systems. This event transitioned a supply chain attack from being a significant state-sponsored effort to a reasonable vector for everyday criminal activities.

## Why Are Supply Chain Attacks So Effective?

Supply chain attacks have successfully infiltrated and disrupted networks, regardless of the bad actor's goal. These new threats have distinct advantages over traditional attacks:

1. **Supply chain attacks can come from anywhere, often inside the normal boundaries.**
2. **History is not a guide. Most attacks are new to victims.**
3. **Lack of visibility and awareness of the supply chain prevents the preparation of attacks.**



Interos Inc. Ecosystem Powered by Interos

Map | Your Ecosystem

Viewing 5855 organizations in your ecosystem

6,235 companies

Figure 1. Interos ecosystem map

See Everything. Do Anything.™

## With Interos, you will be able to:

- Identify your sub-tier suppliers to the $N^{th}$ tier
- Monitor your suppliers and sub-tier suppliers against multiple risk factors
- Identify your top at-risk suppliers
- Identify suppliers with solvency or liquidity issues
- Avoid suppliers who operate in restricted countries or industries
- Receive alerts when status changes
- Evaluate alternative suppliers
- Read news and insights about your suppliers

## How Interos Empowers the CISO

The Interos Operational Resilience Platform empowers the Chief Informational Security Officer (CISO) to respond to supply chain attacks, audit and monitor their supply chain, and improve supplier vetting.

**Incident response driven use cases – Protect your organization from cyberattacks originating from within your supply chain**
CISOs must quickly and confidently respond and mitigate when a new attack happens:

- Quickly determine if a supplier is in the organization's extended supply chain.
- If so, how is that supplier connected in their supply chain?
- What is the risk to the organization?
- How to best mitigate the threat – patch, reposition or remove?

Since supply chain attacks can come from anywhere without warning, being adequately prepared to mitigate them quickly is the best approach.

**Compliance-driven use cases (regulatory, industry standards) – Assess suppliers to ensure compliance**
When a supply chain audit or supplier monitoring is required, the CISO must:

- Find all suppliers in the supply chain that violate U.S. Federal and European Union (EU) sanctions and restrictions resulting in fines and loss of business contracts (i.e., Office of Foreign Assets Control (OFAC), Section 889, etc).
- Find all suppliers in the supply chain that have poor cyber standards resulting in lost business and possible cyberattacks (i.e., European Commission Digital Operational Resilience Act (DORA).
- Proactively monitor supplier health to find all suppliers with poor cyber and financial scores to prevent compromise in the future.

A lack of visibility of the supply chain prevents the CISO from making improvements. Interos provides that awareness.

**Compliance-driven use cases (internal) – Perform a supplier onboarding review to prevent future problems with suppliers**
These use cases show how Interos can optimize internal processes (e.g., supplier onboarding) by improving efficiency/efficacy:

- Find suppliers with high-risk factors who are likely to be breached and therefore, churn before the end of the contract period.
- Perform initial assessment in hours, not weeks or months, saving time and money for use in the internal onboarding process.

By immediately identifying high-risk suppliers, companies are equipped with data to prevent future disruptions. Through the Interos Operational Resilience Platform companies can therefore improve the overall health of their supply chains.

## About Interos

Interos is the operational resilience company — reinventing how companies manage their supply chains and business relationships — through our breakthrough SaaS platform that uses artificial intelligence to model and transform the ecosystems of complex businesses into a living global map, down to any single supplier, anywhere.

Request Contact

For more information:
www.interos.ai or **+1 703.677.3135**

## Use Cases

**Rapid Response**
Uncover the threat in your extended supply chain in hours, not weeks or months

**Supplier Assessment**
Continually monitor suppliers to prevent surprises and proactively prevent problems

**Supplier Onboarding**
Assess suppliers using standard based approach to uncover hidden issues