Marsh

Defining and uncovering the cyber risks in your digital supply chain

Are cyberattacks against supply chains inevitable? The bad news: Yes. The good news: While it may not be possible to prevent all supply chain cyberattacks, the risk and impact can be potentially managed and minimized.

Why are attackers targeting supply chains?

A supply chain attack is when an attacker gains access to your data through one of your vendors or partners. These types of attacks present cyberattackers with enormous opportunities for exploitation. A successful attack against even a single vendor or supplier can yield sensitive data across multiple organizations.

Supply chain attacks by the numbers

700

organizations were affected by third-party/supply chain compromises in 2020

42 million

individuals were impacted by third-party/ supply chain compromises in 2020

39%

of global business leaders who believe supply chain partners pose a high/somewhat high risk to their organization

43%

of leaders who report no confidence in their ability to prevent third-party cyber threats

430%

increase in attacks against the software supply chain between 2019 and 2020

What is a digital supply chain?

A digital supply chain can be defined as:

1. The digital aspects of a physical supply chain or a traditional supply chain powered by digital technology.
2. The chain of technology companies involved in the delivery of digital products.

These two definitions overlap, as almost all supply chains can be considered digital — and third-party technology vendors may supply the technology used in the digital supply chain.

It's thus important to understand your vendor ecosystem and how they support your digital supply chain. Do you know who provides the digital products and services on which your company relies? Or any critical products/services, for that matter?

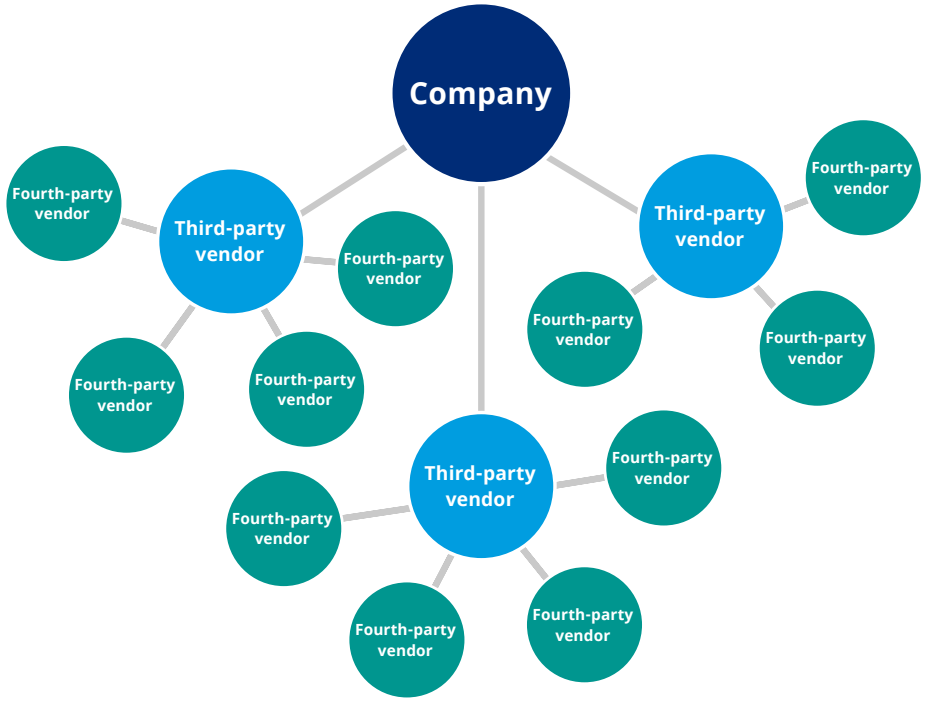
As you look deeper into your digital supply chain, consider potential risks from:

- **Third-party vendor/suppliers**, which include any entities that provide products or services to your organization to maintain daily operations, and/or provide products or services on behalf of your organization (for example, technology vendors and critical component/product suppliers). These third parties can pose a risk to all organizations, especially those that have technology connectivity or access to data.
- **Fourth-party vendor/suppliers**, which are the suppliers of your suppliers. Every company outsources parts of its operations to multiple vendors and suppliers. Those suppliers, in turn, outsource parts of their operations to other suppliers.

The larger your ecosystem is, the bigger your attack surface and potential vulnerabilities are.

Many organizations struggle to understand their complex digital supply chains and the myriad vendor relationships that support their operations — especially those that have access to IT systems and/or data. Regardless of how it's defined, the expansion of a company's digital supply chain brings increased cyber risk.

Third- and fourth-party risk ecosystem



How does this play out?

Consider the digital supply chain risks in the following scenarios, where an organization:

Scenario	Risk	Impact	Example
Uses technology to drive efficiencies in its physical supply chain (digital supply chain definition #1).	A technology disruption halts the supply chain.	First-party business interruption, plus other extra expenses and costs.	Internet of things (IoT) devices are compromised with malware, disrupting a production line.
Engages technology vendors to power day-to-day operations, and has technology connectivity to the vendor.	A technology disruption to the vendor discontinues the company's operations.	Contingent business interruption, plus other extra expenses and costs.	An outage at a cloud provider causes website downtime and prevents order fulfilment.
Relies on technology vendors to power day-to-day operations, and has technology connectivity to the vendor.	Compromising of the technology vendor's products/services impacts the company's network.	Potential cyber incident, including a breach, ransomware attack, or business interruption plus related costs.	A software vulnerability leaves an open door for attackers, enabling them to install malicious code on the company's network.
Entrusts confidential information on customers and employees to a third-party vendor, and is not connected to the vendor.	A breach of the company's confidential information caused by the vendor.	Privacy incident with first- and third-party costs.	Payroll provider suffers a breach of employee information, or a technology vendor compromises customer loyalty information.
Uses a third-party vendor for specific good/services, and does not have technology connectivity to the vendor.	Technology disruption to the vendor hinders the company's ability to generate revenue.	Contingent business interruption, plus other extra expenses and costs.	Network disruption affects a company's ability to receive its product.

What can you do?

As we see more attacks on critical technology vendors and organizations' digital supply chains, it's more important than ever to define what is meant by digital supply chain, how the term is understood within your organization, and what types of cyber risks manifest from your critical third-party vendors and digital supply chain.

While supply chain cyberattacks can't all be prevented, they can be identified and managed to reduce impact. Supply chain resilience can be achieved through identification and understanding of the risks and their potential impact, planning for when an attack happens, and finding the right balance between risk mitigation and risk transfer.

MARSH CYBER CAN HELP

Marsh's robust suite of cyber supply chain offerings includes:

- Third party-vendor risk management framework development.
- Vendor risk monitoring.
- Quantification of digital supply chain cyber risk.
- Incident response and business continuity planning in support of incidents caused by vendors.
- Cyber incident management services, including claims support and proof of loss for digital supply chain cyber incidents.
- Insurance brokerage services designed to address losses caused by vendors and to digital supply chains.

Marsh has helped organizations around the world better understand and manage their supply chain risk. Email cyber.risk@marsh.com to learn more.

About Marsh

Marsh is the world's leading insurance broker and risk advisor. With around 40,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue over $17 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. Follow Marsh on Twitter @MarshGlobal; LinkedIn; Facebook; and YouTube, or subscribe to BRINK.

1166 Avenue of the Americas, New York 10036