Deloitte.

Helping a large industrial manufacturer proactively identify and mitigate supply network disruptions

Operate | Supply Chain Resilience

The challenge

A large industrial manufacturer faced severe supply disruptions during the COVID-19 pandemic. This was further exacerbated by ongoing global events and economic disruptions, leading to significant production inefficiencies and customer order delays.

The client had limited visibility of upstream supply networks and associated risks beyond their Tier 1 suppliers. Additionally, they lacked streamlined processes or strategies for delivering and driving proactive mitigation.

Our solution

Deloitte developed and now runs an integrated Supply Chain Resilience as a Service solution, managing disruptions across the client's global supply chain, illuminating their multi-tier supplier network for deeper visibility, and ongoing risk monitoring.

This includes a supply chain resilience operating model with revised governance and technology to increase internal functional and supplier coordination, to drive more timely and effective responses to disruption.

Ongoing tech-enabled monitoring delivers insights that drive proactive management of risks across several risk domains (e.g., operational, cybersecurity, etc.).

The outcomes

Sample incidents and risk responses

- **Operational**: Quickly found alternative suppliers and sourced additional raw materials after a factory fire was reported in a key supplier. The client responded with agility to honor their planned production schedule.
- **Financial**: Identified and responded to signs of financial distress with a key supplier and the potential impact on material supplies. This enabled the client to take swift action to mitigate the impact of the supplier's eventual insolvency months later.
- **Global events**: Forecasted a disruption in commodities markets caused by alerts of potential political unrest in certain markets. This enabled early supply contingency plans to be put in place with key suppliers who were most susceptible to disruption.
- **Cyber**: Identified a ransomware attack with a supplier and conducted a proactive assessment to determine client exposure and alternative sourcing options to maintain production.
- **Other domains:** Monitors ESG, labor, logistics/freight, natural disasters, commodities, and more on an ongoing basis.

deloitte.com/operate