



somewhat  
different

Complex supply chains are vulnerable and prone to business interruption.  
IT outages are the most critical events that are likely to test supply chain resilience.

## Supply chain risks

The dependency of businesses on stable global supply chains continues to grow in stride with ever-increasing globalisation. The 2011 natural catastrophes in Australia, Japan and Thailand have shown how vulnerable global supply chains have become. For (re)insurers, the major earthquake in Japan in March 2011 led to substantial claims from Western companies with operations or suppliers in Japan suffering from contingent business interruption. Products such as semi-conductors were delayed not only because of production stops, but also because shipping routes and harbours were not readily accessible. This affected industries globally that rely heavily on electronic components, such as automotive, computers or electronic devices.

Supply chain vulnerability has developed over the last decades in line with evolving processes that promoted the ideas of “lean manufacturing” and “just-in-time” supply. There has also been an increasing trend to source globally in order to further reduce costs along the chain. Supply chain resilience has not only been tested by natural catastrophes but also by the global economic crisis, the swine flu pandemic of 2009 and 2010, and the volcanic eruption in Iceland of 2010 with continued interruption of global air traffic.

Business interruption continues to develop into a major issue. Already business interruption claims on average are substantially higher than related average direct property damage claims. Recent industry surveys show that supply chain risks are rated as a top peril by industry leaders. Nevertheless, the majority of industries seem to have no full overview of their supply chains.

Interviews with key industry figures also found that many such respondents had experienced supply chain interruptions already and that in many cases these disruptions were not resolved smoothly. Affected parties suffered from productivity losses, higher costs, drops in revenue, but also from damage to reputation. Unexpected IT outages as a result of cyber-attacks and data breach are assumed to be the biggest threats for the near and mid-term future.

Companies can address this risk of financial loss either through business interruption insurance or contingent

business interruption insurance. Business interruption (BI) insurance covers lost profits after a company’s own facility is damaged by an insured peril (e.g. fire, natural catastrophe), while contingent business interruption (CBI) insurance covers lost profits if an insured peril does not affect over the policyholder’s own facilities but rather its critical supplier or a major customer. Business interruption and CBI losses typically account for 50% to 70% of catastrophe losses.

BI and CBI insurance typically only cover supply chain disruptions resulting from a physical loss or damage to insured property. Consequently, standard BI policies do not cover other disruptive events without a physical loss. However, numerous disruptive events may lead to BI without a causative physical loss, e.g. failure in service delivery by a supplier, product quality incidents, strike, riots, outbreaks of disease, outages of IT and communication systems, or cyber attacks. Of all such disruptive events affecting supply chains, IT outages appear most critical. To bridge this insurance gap, alternatives to traditional BI and CBI coverages now are available.

Supply Chain Interruption (SCI) insurance products gradually are being introduced in the market. Historically, these products have gained traction slowly due to limited capacity, high prices and prohibitive risk data requirements. Most markets do not provide all risks policies but offer named risks covers with restrictions and exclusions.

One of the main reasons for (re)insurer reluctance in offering SCI policies is the critical issue of risk accumulation. Whilst major parts of the supply chain are unknown (re)insurers attempt to mitigate their accumulation exposure.

For risk evaluation it is necessary to analyse the interdependencies of different supplier levels (1st tier, 2nd tier, 3rd tier) in as much detail as possible. Essential details include in particular the location of suppliers’ facilities and the extent of business continuity plans the policyholder has in place to remain operational if faced with a disruptive event. Transparency and a deeper knowledge of supply chains are necessary to create tailor-made solutions.