# Does Your Supply Chain Harbor Hidden Risks?

## Proactive strategies to reduce risk in the Supply Chain

**Victor Sordillo, PE, CSP**
Senior Vice President,
QBE Global Risk Solutions

Made possible
QBE

### What Creates Supply Chain Risk?

Since the 1980s, globalization – the increased interdependence of large multinational and smaller domestic companies on international labor, raw materials, production, warehousing, distribution and commercial sales – has amplified supply chain risk in ways both predictable and surprising. Moving raw materials and finished products long distances (often from one end of the globe to the other) creates an expected increase in risks. Given that the multitude and variety of risks are becoming more predictable, the leadership of multinational and domestic companies can benefit from taking a closer look at how global interdependence affects each link of their supply chain.

### A Closer Look at Supply Chain Risk

Supply chain risks are legion, especially given the backdrop of globalization. Further, there are any number of elements within each industry that can prove problematic under the right conditions – or, for that matter, under normal conditions. With that in mind, here are seven key areas of risk that tend to affect multinational and domestic companies – both the companies themselves, as well as their sources of pre-manufacturing materials, and their many suppliers.

*Recent factors exacerbating supply chain risk*

- **Globalization**
- **Just-in-time delivery**
- **Climate change/extreme weather events**
- **Increased social/environmental activism**

## Manufacturing Site Safety

Multinationals and domestic companies need to be aware of their suppliers' site conditions. There are two distinct reasons for this. Not only could site risks halt production, should their suppliers fail to deliver but, they could also damage the reputations of the companies they supply.

Companies would be well-advised to learn the "ins and outs" of their energy sources; checking for reliability, and locating alternate sources that could be employed during emergencies. Energy in foreign countries – i.e., electricity and natural gas sources – may not be as dependable as we are accustomed to in the U.S.

Energy concerns should also come into play whenever a company decides to expand to a new site. While local labor laws, government tax breaks, and extreme weather issues are all important considerations, a reliable and sufficient energy source is fundamentally important when selecting a new plant site.

In addition, fundamentals of property protection should not be ignored. Some areas that need to be assessed concern fire protection, security, building construction and the age of the building. Water supply for fire fighting is not abundant everywhere; crime rates and gang-related violence can be an issue; and many developing nations do not have or enforce building codes affecting structural integrity and safety.

## Labor Conditions

When companies outsource labor to developing nations, a critical proactive risk reduction strategy involves evaluating foreign plant worker conditions – preferably by sending a representative in person – to be certain those workers are not subjected to unsafe facilities, longer-than-normal hours, and that those workers are adults and not children. Not only can all these elements present a reputational threat, they can also lead to plant close-downs due to violations and, in some instances, labor strikes. Both outcomes will lead to a disruption in production, which can in turn affect customer loyalty and result in a decline in sales and income.

## Quality Control

Multinationals and domestic companies have on-site oversight with regard to the quality of their products, but when they outsource part or even all of their production, their ability to control product elements or whole-product quality may disappear. One common but faulty expectation of many multinational companies, in particular, has been the assumption that the products they order and receive will match the sample product that sold them on ordering from a particular foreign manufacturer in the first place. All too frequently, however, the sample and the actual shipped product are two different things, and, as a result, companies have found themselves recalling spoiled or contaminated food products, replacing defective car parts, and, in one

instance, suffering a complete ban of their recreational product because its defective battery burst into flames within minutes of use. Add to that the fact that, in some foreign countries, multinationals and others have no legal recourse, no possibility of subrogation, because those countries assert their "sovereign immunity" from claims.

## Business Reliability & "Coopetition"

Equally important to manufacturing concerns are their suppliers' sources of supply. In other words, it isn't enough to check the reliability and financial health of companies supplying raw materials and component parts. Their suppliers should also be analyzed for potential risks. In a tangentially related example, the sole manufacturer of a brake component used by virtually all car manufacturers experienced a plant-destroying fire. But as there was no back-up supplier for that part, production was slowed down for months throughout the auto industry.

A related scenario can occur when a manufacturer depends upon highly customized machinery to produce its products. If that machinery breaks down, there may be no way to continue production until it is fixed, or a new machine is made. The obvious risk-mitigating answer is to have critical parts and even substitute machines on hand, or at least an alternative method for producing the product. If possible, it's wise to establish a mutual agreement – whereby your company and a competitor will back each other up, should either be faced with an emergency.

*The obvious risk-mitigating answer is to have critical parts and even substitute machines on hand, or at least an alternative method for producing the product.*

## Cyber-Security

Since every aspect of manufacturing is now highly automated or computerized, the threat of sabotage from cyber-criminals is very real. So it's critical for business leaders to minimize access to their computerized operations; in particular, to guard their computer systems and/or areas of high security (client lists, product designs); monitor their security procedures on a regular basis; and be sure to install the most recent versions of fire wall and encryption technology.

Another area in which companies can be vulnerable to cyber-crime involves employees not understanding that an infected thumb drive, say, or a weak password can provide hacking opportunities for criminals looking to access the company's server. This risk can easily be reduced by providing computer safety trainings, sending out regular reminders, and installing a system of checks and balances – to ensure that cyber-crime is taken seriously by employees at all levels.

As the Internet of Things (IoT) expands, so too do supply chain-related cyber risks. Software embedded in IoT products at different tiers of the supply chain can pose security flaws that ordinary functionality testing may not reveal. The security of these components is typically weak and leaves an open avenue of attack for hackers.

## Packaging & Transportation

Manufacturers would do well to investigate both the shipping routes and the packaging procedures their raw materials suppliers and product distributors employ. In some developing countries, a lack of packaging and shipping standards can result in products or manufacturing supplies being badly damaged en route.

A badly wrapped shipment of needed manufacturing supplies, for example, sat for a week on the tarmac of a small airport that was flooded repeatedly with heavy rains. By the time this shipment arrived, the supplies were useless, and the production schedule was subsequently delayed. As a result, it's important to know where your materials and products are at every stage of the shipping process; that they are stored in secure, guarded, fire-protected facilities; and that they are packaged to survive any number of conditions they might be exposed to. In other words, you can't assume that the shippers have thought of these things and taken care of them. It's more than likely that they haven't.

A related risk comes from product hijacking or piracy – a common occurrence when high-value products travel across borders and thieves have an opportunity to bribe officials; or when truckers must stop for the night, making their cargo more vulnerable to theft. To mitigate this risk, it's a good practice to vary shipping routes; use unmarked vehicles (don't advertise the valuable products inside with a brand name plastered on the side of the truck); and be sure there are secure locks, GPS monitoring devices, and alarms, as well as other more sophisticated devices, to foil potential thieves.

## Regulatory Risk

In the U.S., one hard-to-predict risk is how the rules and regulations governing the production and sale of products will change over time. More than three decades ago, for instance, after passage of the Child Safety Protection Act, toy manufacturers were told that all the parts for every toy manufactured for children three years old and younger had to be a certain size – to prevent choking that could, in turn, be fatal. As a result, companies rushed to retool their machinery, recall older product not yet sold, and warn the public about the choking risk, if they'd purchased earlier versions of their toys. Since many nations have yet to adopt similar regulations, diligence must be maintained to ensure that all imported products or components meet the U.S. standards of safety.

## Strategies to Address Supply Chain Risks

Considering the complex and evolving risks inherent in today's typical supply chain, especially when sourcing from abroad, manufacturers must develop an overall strategy for evaluating and mitigating risk. Large global manufacturers can afford to have in-house risk managers to lead this task, partnering with insurance brokers and carriers, and conducting business continuity planning for a wide range of scenarios. Furthermore, their output volume often gives them enough perspective or experience to identify weak points.

Mid-size and small manufacturers, however, may not have the scale to support a thorough in-house evaluation of supply chain risks, and lower output volume compared to large companies means they have fewer opportunities to learn through experience – until it is too late. For these companies, working with an expert broker and insurance carrier that specialize in serving manufacturers and have the perspective of working with many similar companies is especially important.

Manufacturers will want to consider not only the quality of insurance coverage as it relates to supply chain risk but also the skill and capabilities of the risk assessment team, often called the loss control team. As part of the underwriting process, the risk assessment team will identify the potential for loss related to the coverage and recommend steps to reduce it. The process requires detailed knowledge and the best risk assessment teams will often include licensed engineers for each category of risk. If the supply chain extends internationally, the manufacturer should also be confident that the insurance carrier has the resources to evaluate the suppliers in the foreign countries.

**Supply chain risk assessment checklist**

***Supplier site safety***

- ❑ Fire, water damage
- ❑ Natural disaster
- ❑ Power outage
- ❑ Theft
- ❑ Cyber

***Supplier site labor conditions***

- ❑ Worker safety
- ❑ Worker hours/ working conditions
- ❑ Child labor
- ❑ Strike threat
- ❑ Political stability

***Supplier quality control***

- ❑ Defective design
- ❑ Insufficient quality control
- ❑ Tainted raw materials

***Supplier responsibility***

- ❑ Ability to subrogate claims – foreign government ownership/immunity
- ❑ Insurance adequacy

***Supplier business health***

- ❑ Bankruptcy potential
- ❑ Corruption

***Packaging***

- ❑ Breakage or spoilage
- ❑ Weather/environment resistance

***Transportation***

- ❑ Accidents
- ❑ Theft
- ❑ Security of temporary storage points
- ❑ Route disruption due to catastrophes, port strikes

***Cyber risk***

- ❑ Network security
- ❑ Employee susceptibility
- ❑ Embedded code in product components
- ❑ Hardware vs. software

***Regulatory risk***

- ❑ U.S. vs. Foreign
- ❑ Quarantine

**Key insurance coverages and consideration for supply chain risk**

## Contingent Business Interruption and Business Interruption

Contingent business interruption coverage plays a central role in protecting business income from supply chain risk. Offered as optional coverage in a commercial property policy, it typically covers lost income as a result of loss to a supplier's or recipient's property that impairs delivery of the promised product. It is important to understand specifically what perils are covered by the policy. Usually, the coverage is an extension of whatever perils are covered in the manufacturer's property coverage. But what if the perils at the supplier's location are very different from those at the manufacturer's location? For instance, the manufacturer may have decided to forgo flood or earthquake coverage because those risks are extremely low at their locations. The supplier, however, may be in an area highly exposed to flood or earthquake loss. Power outages, labor strikes, and cyber attacks are other risks often overlooked in the policy terms.

*Contingent business interruption coverage plays a central role in protecting business income from supply chain risk.*

Contingent business interruption policies are frequently limited to named locations of the suppliers. While coverage can also extend to unnamed locations, insurance companies are understandably much more selective about assuming risks for locations they cannot inspect. They may impose stricter terms, charge a higher rate, and be unwilling to offer the same amount of coverage as they would for named locations. To secure the best coverage and rates, risk managers will likely find it is well worth the effort to understand and document all the locations of their suppliers for inclusion on the policy – and to keep the information up to date.

In many cases, manufacturers not only depend on components and materials coming from another company. They source goods from other locations that they own. These locations can introduce many of the same risks into the supply chain that outside suppliers do. In such cases, business interruption coverage protects the manufacturer against lost income if an incident at the other company location disrupts the supply chain. If that location is in a foreign country, the manufacturer should make sure that the policy territory includes it.

## Transit and Inland Marine

Manufacturers should also pay special attention to how the goods are insured while in transit. They should understand the coverage secured by the supplier and shipping company, and how it interacts with their own insurance. Sufficient limits should be in place to cover the value of the goods.

Importantly, the manufacturer should know exactly when it takes ownership of the product being shipped to them, which might not be when the product reaches the manufacturing facility but at a point along the transportation route, such as a port or customs facility. At this point, transit coverage becomes necessary to insure the goods on a first-party basis. Transit coverage also applies when a manufacturer ships goods it produces between locations it owns as well as to customers, before the customers take possession.

## Product Liability and Product Recall

In today's increasingly litigious and regulated environment, manufacturers should strongly consider adding product liability and product recall insurance to their commercial general liability policy to address supply chain risks. Should use of their product result in property damage, personal injury, bodily injury or death, manufacturers can be held liable – even if the cause is a defective part sourced from another company.

Furthermore, such incidents, as well as regulatory changes, could result in costly product recalls. In addition to the lost value of the recalled products and the prospect of business interruption, executing the recalls can involve costs to broadly communicate the recall, ship and dispose the recalled product, and minimize and then repair damage to the manufacturer's reputation. To guard against this risk, manufacturers should work with their brokers to understand the breadth of coverages offered by the insurance company for product recall coverage in conjunction with product liability.

## Errors and Omissions

Errors and omissions (E&O) coverage is another important consideration to enhance protection needed by manufacturers. As previously stated, product liability applies in cases of property damage, personal injury, bodily injury or death. But end users of a product may also sue the manufacturer if use of a product results in financial harm even if bodily injury or property damage has not occurred. Errors and omissions coverage fills this gap. Superior policies or endorsements will include coverage for damages to a manufacturer's product, work, impaired property or property not physically injured.

## Cyber

Finally, Cyber insurance is playing an increasingly important role in managing supply chain risk, since company connections to the internet and hardware and software powering a manufacturer's systems can be considered a form of supply. Even systems completely cut off from the internet can be compromised by an employee unknowingly plugging an infected USB drive from a third party into a company computer.

The more robust cyber products will provide coverage for a wide range of risks, including: privacy and network security liability; media liability; data breach notification costs; information and communication asset rectification costs; regulatory defense and penalty costs; public relations costs; forensics costs; credit monitoring costs; cyber business

interruption; and cyber extortion. The best offerings will also offer access to specialized tools and services that help companies assess cyber risk and prevent and respond to incidents.

In addition to their own cyber insurance policies, manufacturers should ask suppliers about the cyber protection they have. As product components increasingly have embedded code and cyber functionality, manufacturers will want indemnification against flaws and vulnerabilities in those components, should customers and other third parties sue for compensation as a result of cyber related losses associated with that component. The solution often involves naming the manufacturer as an insured on the supplier's cyber policy. The language of the policy, however, must be constructed so that the manufacturer is still allowed to hold the supplier liable for damages if the supplier suffers financial failure due to a cyber incident. In many cases, policy exclusions prevent one named insured from collecting damages from another named insured on the policy.

## Proactive Supply Chain Risk Management

The global interdependence of operational supply chains in the 21st century can be a source of profit for multinational and domestic manufacturers, as well as the underlying cause of risks that were relatively unknown in the mid-to-late years of the previous century.

A proactive response by industry leaders can, however, mitigate many production and distribution risks, and help them prepare judiciously for less-likely risks that may, one day, occur. Not responding to the clearly visible as well as the more uncommon risks is not an option – given the complex way that goods now travel the globe to reach their markets and buyers.

*Insurance checklist for supply chain risks*

- ❑ **Contingent business interruption**
- ❑ **Business interruption**
- ❑ **Transit**
- ❑ **Inland marine**
- ❑ **Product liability**
- ❑ **Product recall**
- ❑ **Errors and omissions**
- ❑ **Cyber liability**

---


**About the Author**

Victor Sordillo serves as Senior Vice President of QBE North America's Global Risk Solutions Unit, planning, directing, and executing QBE's loss control vision and strategies by developing long-range business objectives, establishing a strategic framework to guide regional operations, and directing risk management practices that help reduce losses.

He serves as a Trustee to the New Jersey Manufacturers Extension Program (MEP). This non-profit organization was established by National Institute of Standards and Technology (NIST) as a private public partnership to support and build manufacturing in the USA. Since 1988, MEP has worked with more than 86,000 manufacturers producing $96.4B in sales, $15.7B in cost savings, and more than 797,994 jobs.

**About QBE North America**

QBE North America is part of QBE Insurance Group Limited, one of the largest insurers and reinsurers worldwide. QBE NA reported Gross Written Premiums in 2015 of $4.6 billion. QBE Insurance Group's 2015 results can be found at qbena.com. Headquartered in Sydney, Australia, QBE operates out of 43 countries around the globe, with a presence in every key insurance market. The North America division, headquartered in New York, conducts business through its property and casualty insurance subsidiaries. QBE insurance companies are rated "A" (Excellent) by A.M. Best, and "A+" by Standard & Poor's. Additional information can be found at qbena.com, or follow @QBENorthAmerica on Twitter.


*https://www.washingtonpost.com/business/reconsidering-the-value-of-globalization/2015/04/24/7b5425c2-e82e-11e4-aae1-d642717d8afa_story.html*

*https://ourfiniteworld.com/2013/02/22/twelve-reasons-why-globalization-is-a-huge-problem/*

*http://www.triplepundit.com/2015/04/12-business-and-sustainability-risks-that-can-disrupt-modern-supply-chains/*

*https://people.hofstra.edu/geotrans/eng/ch9en/conc9en/supply_chain_risks.html*

*https://hbr.org/2012/06/managing-risks-a-new-framework*


* Learn more about ratings guidelines at standardandpoors.com and ambest.com.