

SUPPLY CHAIN RISK MANAGEMENT IN GLOBAL MARKETS

WHITE PAPER

JAN 2021



VIRGINIA ECONOMIC
DEVELOPMENT PARTNERSHIP
INTERNATIONAL TRADE DIVISION

OLD DOMINION UNIVERSITY
STROME COLLEGE OF BUSINESS
MARITIME & SUPPLY CHAIN
MANAGEMENT PROGRAM

Table of Contents

I. FROM DISRUPTIONS TO NEW OPPORTUNITIES	4
1. Managing Supply Chain Risk	5
2. Potential Pitfalls in Supply Chain Operations	8
Supplier selection risks (single source).....	8
Global sourcing risks	11
Foreign exchange risks	13
Errors in Incoterms	14
Perils during transportation.....	17
Perils during storage (warehouses and distribution centers).....	19
Inspection failures (pre-shipment and ex-works at a factory)	19
Failure to transfer risks via insurance/errors in insurance coverage.....	20
Cyber-attack risks	20
3. Preparing for the Unexpected in Supply Chain Operations.....	21
Supplier's evaluations	21
Evaluations of reshoring and near-shoring vs. offshoring	22
Monitoring documentation, terms of trade, and terms of payment.....	23
The importance of insurance coverage	24
4. Supply Chain Disruptions	26
Types of disruptions.....	27
Disruption effects.....	27
Mitigation strategies for disruptions	28
Resilience monitoring	30
II. FINAL THOUGHTS	31
III. ADDITIONAL RESOURCES	31

Acknowledgment:

This white paper is a product of collaboration between Virginia Economic Development Partnership (VEDP) International Trade division and Old Dominion University (ODU): Maritime and Supply Chain Management Program (MSCM), Dr. Ricardo Ungo, Director Maritime, Ports and Logistics Institute, and Krista Kubovchik, MSCM program student.

FROM DISRUPTIONS TO NEW OPPORTUNITIES

... Is a "new normal" here to stay? How will these uncertain times alter supply chain operations? Is going global for sourcing needs still worth it? Good situational awareness of potential vulnerabilities, mitigation actions, contingency plans, innovation, and flexibility are the cornerstones of business continuity.

Over the last decade, modern supply chains spanned through the globe reaching unprecedented levels of complexity. These long supply chains that involve numerous suppliers in multiple countries pose a series of challenges to the companies that have them: safety stock vs. lean inventory levels, quality vs. cost, offshoring vs. reshoring, among others.

Risk is intrinsic to any business activity. While eliminating all operations risks is virtually impossible, identifying, prioritizing, and mitigating risks in supply chain planning is imperative for long-term success. The events of the COVID-19 pandemic applied a tough stress test on domestic and global supply chains and brought the concept of resilience to the forefront of supply chain planning. Good situational awareness of potential pitfalls (natural or human-made), mitigation strategies, post-disruption recovery plans, flexibility, and innovation are the cornerstones of business continuity planning (BCP).

This white paper reviews current principles and issues in supply chain risk management and provides tools for identifying, assessing, and mitigating risks. The document presents considerations regarding resilience and the need for robust contingency plans for post-pandemic international supply chain planning.

1. Managing Supply Chain Risk

Some companies start small, without any formal planning for their supply chains, focusing on one specific area of supply chain at a time: warehousing, distribution, transportation, among others. The risks associated with the operational aspects of these components are often overlooked or assessed in isolation. As business grows, its supply chains become more complex, and the risks associated with them are also more challenging. Companies must dedicate time and effort to assess if their current supply chain strategies will successfully cope with short- or long-term disruptions, whether natural or human-made. Risk management becomes an overarching principle in designing a supply chain network and defining the supply chain strategy going forward.

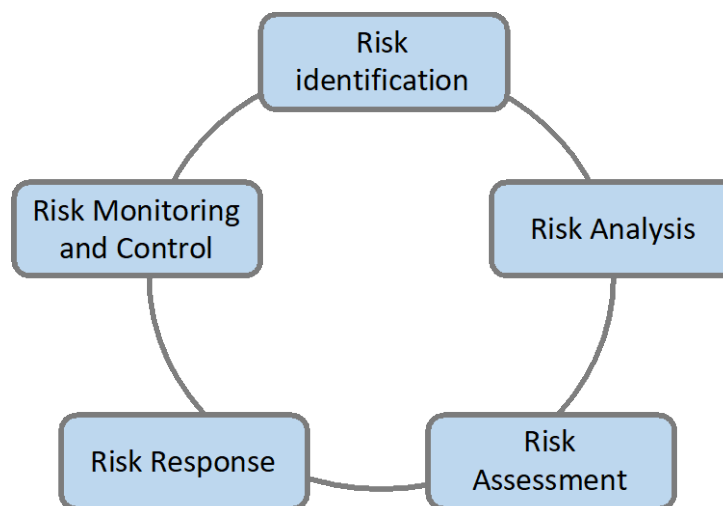


Figure 1. Risk Management Cycle

Risk management implies a continuous cycle of activities described below:

-
-
- a. *Risk identification* focuses on determining critical risks and vulnerabilities associated with each supply chain.
 - b. *Risk analysis* is the next step in determining the likelihood and potential impacts of the risks defined in stage one.
 - c. *Risk assessment* evaluates each risk's expected impact and prioritizes the risks in terms of the firm's strategy.
 - d. *Risk response* implies a specific response to a particular risk. The possible response may include several options such as accepting, transferring, avoiding, or mitigating the risk.
 - e. *Risk monitoring and control* involve continuous monitoring of the changes and evolution of relevant risks over time. As new risks are incorporated in the firm's analysis, the risk management cycle will start again.

The initial step for a supply chain risk manager to undertake will be *risk identification*. The managers in charge of the supply chain or logistics operations need to identify:

- What risks might create a significant loss or disruption to the operations as a whole?
- How severe could the consequences be for company operations?
- How frequently is the risk-initiating event occurring?

Resilience refers to a supply chain's ability to recover quickly from a disruption that affected critical operational performance. Resilience is a delicate trade-off between two components: vulnerability identification and capability development to enable the company to face such vulnerabilities. In other words, the supply chain should have capabilities proportional to the anticipated vulnerabilities to handle the disruption and its ripple effects. The vulnerability assessment includes an estimation of the likelihood of the disruption and the probable magnitude of the impact. The capabilities to handle

the vulnerabilities are the built-in redundancies and the flexibility needed in supply chain operations.

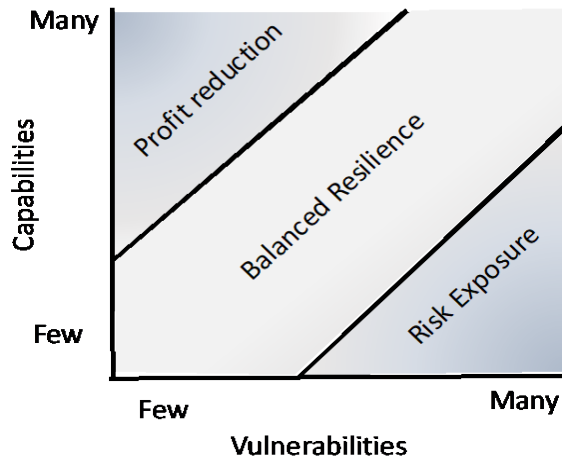


Figure 2. Resilience: Balancing Vulnerabilities and Capabilities
Adapted from: The Evolution of Resilience in Supply Chain Management: A Retrospective on Ensuring Supply Chain Resilience (Pettit, Croxton and Fiksel)

In Figure 2, following Pettit et al.¹, we observe that firms face a balancing act between capabilities and vulnerabilities. If the firm has many vulnerabilities and very few capabilities, then the firm has few safeguards against potential disruptions, creating a considerable exposure to risk. If the firm builds too many capabilities for relatively few vulnerabilities, it operates at a higher-than-necessary cost due to over-investment in redundancies for potential risks and disruptions. Such an approach will make the firm less profitable. The most efficient scenario is to build capabilities proportionally to perceived risks.²

¹ Pettit, T.J.; Croxton, K.L. and Fiksel J. The Evolution of Resilience in Supply Chain Management: A Retrospective on Ensuring Supply Chain Resilience. *Journal of Business Logistics*, 2019.

² For more about the concept of capability coherence, please see The Coherence Premium, P. Leinwand and C. Mainardi, *Harvard Business Review*, June 2010.

2. Potential Pitfalls in Supply Chain Operations

This section covers the most common risks in supply chain operations that can impact a business. These should be taken into account in comprehensive supply chain risk planning. Figure 3 shows nine of the most common risks affecting business operations.

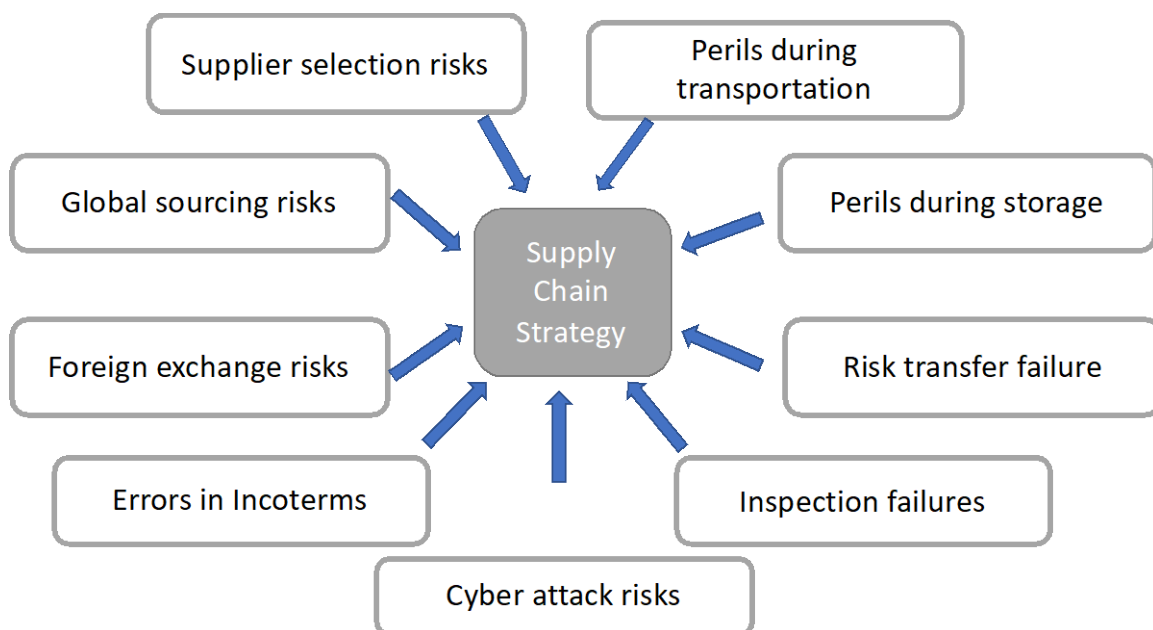


Figure 3. Most Common Risks in Supply Chains

The following sections will address nine of the most common risks in supply chains:

Supplier selection risks (single source)

Supply chains have become increasingly efficient and complex over the past decade. However, the pursuit of these efficiencies and financial gains/profit margins

has generated greater over-reliance on specific geographical regions and a narrower supplier base.

Often, companies rely on single-source suppliers for some of their core components. Single sourcing is defined as the procurement of materials or products from one selected supplier. Although usually there are multiple sources for most supplies, the procurement department may choose to favor a single supplier for various reasons, including:

- a. Desire to establish a strategic alliance with the supplier.
- b. To reduce the variability in the quality levels when using multiple suppliers.
- c. To obtain a lower cost by concentrating volume in one supplier, taking advantage of economies of scale.
- d. The volume needed is too low to be split among several suppliers.

Single sourcing is different from sole sourcing as the latter provides unique components or products that cannot be procured from any other supplier. An example is if the supplier holds the patents to the product or process. Although utilizing a sole source supplier presents the same advantages as a single-source supplier, the risks of a significant disruption to business activities are inherently higher when using a sole supplier because switching to an alternative supply source is more complicated. It is imperative to monitor tier 1 and tier 2 suppliers, mapping the geographical source of supplies and alternative options for each supply chain component, including transportation, delivery options, and warehousing.

Some of the risks associated with utilizing a single or sole source supplier include:

- Capacity limitations when facing increased demand
- Ripple effects throughout the whole supply chain due to disruptions in the single supplier operations

-
-
- Greater dependency between the importer and the supplier
 - Increased vulnerability for supply chain performance
 - Lack of competition
 - A competitor can buy out a single/sole supplier
 - Clients' awareness of a company's reliance on one single supply source.

To overcome the weaknesses of the single-source approach, a company should:

- Review the current sourcing strategy considering the needs for supply chain performance
- Map the supply chain to help visualize potential ripple effects
- Secure at least one backup source for core components
- Engage in proactive monitoring of supply chains
- Review supplier's contracts to consider alternate arrangements in case of a disruption
- Work with the supplier to develop contingency plans in case of disruptions or problems.
- Increase the supply chain visibility in order to identify anomalies
- Identify the financial implications of a potential supply chain disruption, including potential mitigations by insurance policies (e.g., contingent business interruption, supply chain coverage). For more information about insurance coverage, please see Page 22 for "The importance of insurance coverage."

Box 1: Disaster in Fukushima

In March 2011, the devastating tsunami and nuclear disaster that followed in Fukushima Plant, Japan, severely impacted a number of supply chains on a global scale. Companies such as Toyota, with lean manufacturing and reliance on minimum inventories (reduced costs of handling and storing), learned lessons about the lack of resiliency in their supply chains. Five hundred parts came into short supply, which severely limited Toyota's production capabilities for four months. The company's sales dropped as a result of this disruptive event.

However, some companies, such as Apple, had multiple suppliers in Japan and other countries and were able to recover quickly. The events of 2011 prompted Toyota to develop its RESCUE (Reinforce Supply Chain Under Emergency) system that monitors more than 650,000 suppliers. IBM developed its TRA (Total Risk Analysis) system that collects data from 53 countries on multiple dimensions. That tool came in handy during the 2011 Fukushima disaster, allowing IBM to reshuffle its suppliers and structure the backup plans within hours. Although these are examples of lessons learned by large companies, businesses of any size can glean important insights from these experiences.

The essential task of establishing a sourcing strategy is to determine the right number of suppliers for each product component and the evaluation criteria for selecting the suppliers. In recent years, companies have moved away from single sourcing, as disruptions with that supplier may bring their operations to a complete halt.

Global sourcing risks

The decision to source locally, nationally, or globally is pivotal to a company's supply chain strategy. It will affect its profitability, competitiveness, and growth potential. Over the last few decades, domestic and global supply chains became lean by optimizing inventory levels and became more complex through specialization. Global sourcing has surged due to trade liberalization, new information technologies, more

efficient transportation networks, geographical specialization, and improved quality of materials sourced internationally. Simultaneously, these drivers made longer, leaner supply chains more vulnerable to external shocks.

Global supply chains provide access to a wide range of international providers, various consolidation options for smaller volume shipments, better interactivity, and better visibility, thus maintaining an attractive sourcing strategy.

The cost-effectiveness of sourcing globally should never be the sole factor in a company's decision-making. Other factors, including quality of the supplied components, reliability of manufacturing, and political and socio-economic risks in the origin location, should be factored into the sourcing strategy. The table below lists some of the common reasons for and challenges of sourcing globally.

Reasons	Challenges
<ul style="list-style-type: none"> • Largest variety of suppliers (supplier base) • Largest variety of products • Possibly lower cost • Possibly better quality 	<ul style="list-style-type: none"> • Supplier selection is more complex • Longer supply chains and lead times • Handling different currencies, import procedures, and cultures • Political uncertainty • Quality consistency • Vulnerable to disruption risks

Figure 4. Common Reasons for and Challenges of Global Sourcing

To minimize the risks of global sourcing, companies should implement:

- Comprehensive supplier evaluation systems during the selection stage and ongoing performance measurement
- Supply chain mapping, monitoring suppliers and their locations, and the location of their suppliers (Tier 1 and Tier 2 suppliers at a minimum)

-
-
- Effective communication and relationship building (investing in supplier relationship management software, establishing supplier rewards programs, among others.)
 - Contingency and risk management plans
 - Demand monitoring and forecasting
 - Appropriate insurance coverage

Monitoring and managing all possible risks associated with global sourcing may be costly. The least a company should do is identify the risks, prioritize those risks, work with the supplier base to eliminate "knowledge gaps" about those suppliers, and develop mutually agreeable contingency plans.

Foreign exchange risks

U.S. importers need to manage exchange risk exposure when sourcing supplies internationally. This exposure comes from the exchange rate fluctuation between the time the purchaser and supplier enter into a contract and the time the contract is paid. For example, a U.S. importer issues a purchase order for spare parts from a European supplier, and the contract is in Euros. In this case, there will be an exposure to risk due to the fluctuation in the U.S. dollar/Euro exchange rate between the time the purchase order was placed and the time the importer pays for the supplies.

The exchange risk can be either retained or hedged. If the firm decides to retain the exchange rate risk, it will absorb the impact of the exchange rate fluctuation. Importers with little exposure or firms that do not have a clear policy for international currency transactions typically operate in this way.

Alternatively, the firm might decide to hedge the exchange rate risk. There are two possibilities when considering the hedge:

- a. To evaluate the risk on a case-by-case basis, taking into account the currency to be used in the transaction, the total amount of the

transaction, and the exchange rate forecast between the foreign currency and the U.S. dollar.

- b. To set a policy for all shipments that require foreign currency.

For the hedge, forward contracts or option contracts can be utilized. In forward contracts, the exposure is managed through a forward market for currencies. In option contracts, the exposure is managed using the option market for currencies. Another possibility is to handle the exposure through the banking system in a foreign country. Additional resources related to foreign exchange hedging options can be found in the Additional Resources section.

Tip - If the contract amount is significant, the best course of action for the importer is to manage the exchange rate risk by hedging. This will not eliminate the risk exposure, but controlling the risk involved in the shipments' financial transactions will help.

Errors in Incoterms

Another potential risk when sourcing internationally concerns the terms of sale, also known as Incoterms. The International Chamber of Commerce defines Incoterms. Incoterms are internationally recognized rules that stipulate sellers' and buyers' responsibilities in international transactions. A summary of the 11 Incoterms 2020 is shown in Figure 5. (For more detailed information, refer to [ICC Incoterms 2020 rules](#)).

Errors are common when using incoterms and can create significant exposure for a company purchasing from a foreign supplier. Here are a few examples of these situations.

- a. One of the most frequent mistakes is using the FOB (free on board) term with an air shipment or inland point. This is a case of a wrong rule choice. FOB traditionally is used only with ocean shipments, and applying it when the final destination is an inland point can lead to

significant ambiguities and risk exposure if the appropriate amount of insurance coverage is not obtained.

- b. Another common mistake is using the CIF (Cost, Insurance, and Freight) term without ensuring that the seller's insurance matches the commercial contract requirements. CIF requires that the seller provide only a basic level of insurance and, in most cases, is not enough insurance for containerized cargo or manufactured goods. With too little insurance, the buyer will have significant exposure if the cargo is damaged or lost during transportation. (For more information, please refer to "The importance of insurance coverage" section)

The most crucial aspect for the importer is to fully understand the terms of sale for each transaction. The importer should be aware of the obligations, risks, and costs involved with the importing transaction.

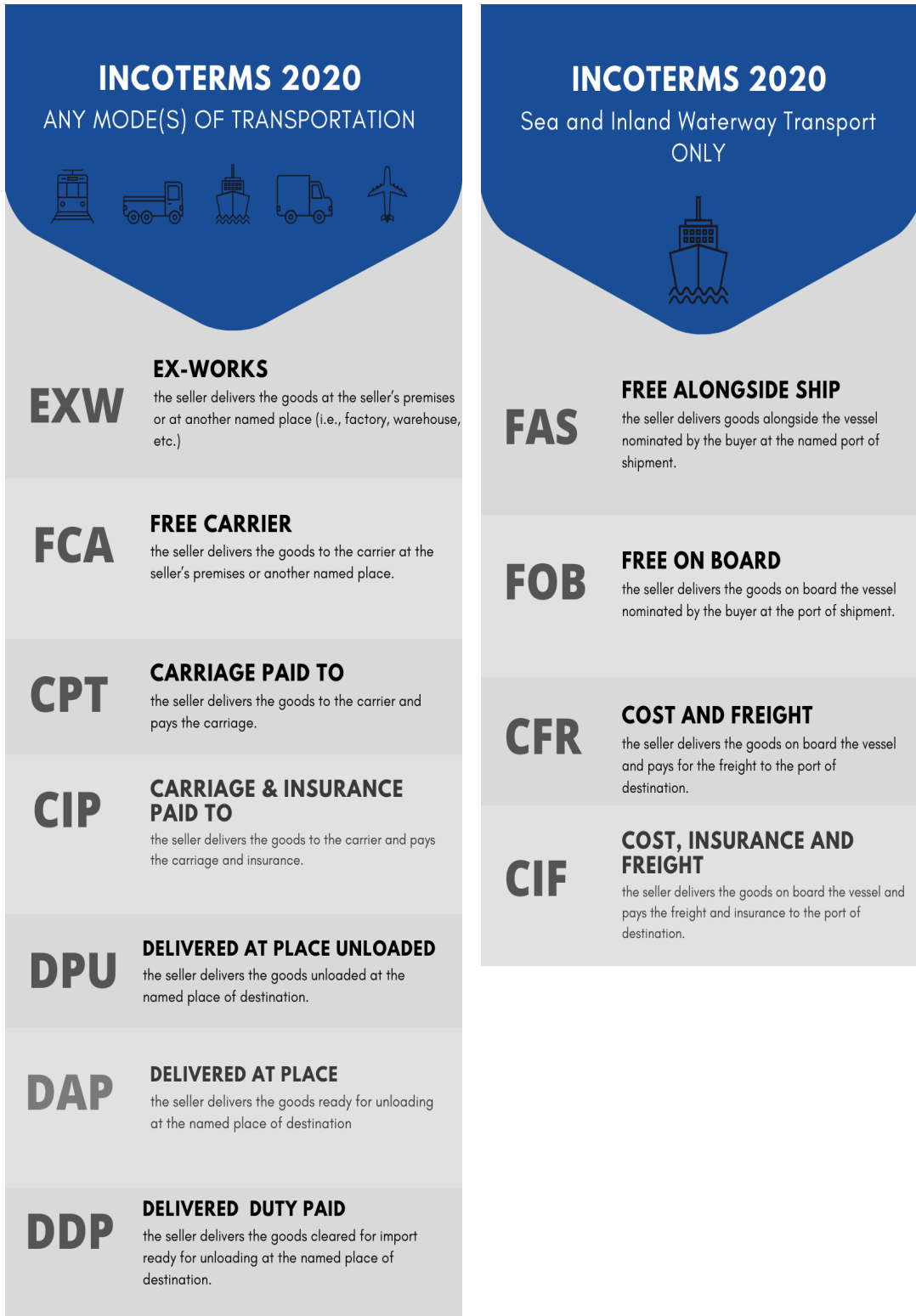


Figure 5. Incoterms 2020 (Source: International Chamber of Commerce (ICC))

Perils during transportation

There are many potential risks to cargo during ocean transport. The most common are:

- a. Water/waves damage. In rough seas, waves can damage cargo or containers on board. Water can also wash overboard into the ship and slowly infiltrate cargo containers.
- b. Cargo movement damage. Cargo can also be damaged due to the ship's movements. A container ship's lash bars can fail in stormy seas, causing stowed containers to collapse.
- c. Theft. The risk of theft is present whether on shore, during drayage movements, or onboard the ship.
- d. Fire. The ability to fight fire on container ships is limited. Fires are frequently declared general average by the shipowner. (For more information, see Box 2).
- e. Cargo lost overboard/jettison. In rough seas, cargo can be lost because the container or crate goes overboard. The ship crew can jettison some cargo or throw it overboard to lighten the weight of the ship during bad weather. (For more information, see Box 2).
- f. Sinking and stranding. This possibility covers the cases of stranding due to a broken engine and tilting damaging the vessel's cargo.
- g. Diverted cargo delays. Due to bad weather or a broken engine, the vessel might need to change the route. Therefore, the cargo will need to be diverted to another vessel or route, causing delays in delivery, or the cargo failing to reach its final destination.

Air transport also poses a risk to cargo. These are some of the most common:

-
-
- a. Cargo handling. While cargo is being handled prior to loading on the plane or after unloading, perhaps from an airport warehouse to the airplane, it is at risk of being damaged.
 - b. Cargo movements. The airplane may experience significant turbulence or speed changes during the flight, causing damage to its cargo.
 - c. Theft. Air cargo is especially vulnerable to theft due to the typically high value of most cargo transported by air.
 - d. Water damage. Water damage can occur if the cargo is left exposed to the elements, most likely before loading onto the airplane and after being unloaded.
 - e. Changes in temperature and atmospheric pressure. Airflight involves extreme temperature changes, from conditions at takeoff to those at the highest elevations. These fluctuations can damage cargo, particularly if the aircraft is only partially pressurized.

Cargo is also subject to risks when being transported by rail or truck. Some of the most common risks include:

- a. Theft. The risk of theft is greater during the loading and unloading of cargo.
- b. Collision. Collisions on roads and highways are frequent and can damage cargo during transport.
- c. Derailment. While train derailments are not common, these events do occur and can bring significant cargo losses.

Perils during storage (warehouses and distribution centers)

Cargo is at risk not only during transport but also while being stored. There are many types of perils that can occur during storage. Some of the most common risks include:

- a. Fire. Fire at a warehouse or distribution center represents a significant risk to cargo.
- b. Theft. Theft represents a significant risk for warehouses.
- c. Flooding. Ruptured pipes or flash floods can affect goods stored at ground level.
- d. Power outages. The outages can have a significant impact on cold storages.
- e. Cargo handling. Incorrect loading and stacking can cause significant damages to merchandise.

Inspection failures (pre-shipment and ex-works at a factory)

Inspections are a valuable tool for importers in terms of verifying conformity versus standards and product specifications. This is especially true when considering agricultural products, high-value goods, or complex technical specifications. These inspections are performed prior to the shipment or ex-works at the supplier's facility. In general, this would be the final opportunity for a corrective action before the goods are shipped. In most cases, importers cover the inspection costs, whereas the costs associated with presenting the goods for inspection are covered by the exporter. A typical inspection includes aspects such as verification of quantities and quality, revision for defects, compliance with technical specifications, among others. For containerized cargo, seals are typically applied when the inspection has been done. Failures in inspections or not performing inspections at all might imply huge risks for the importer. These risks include penalties, customs delays, and even the need to review or re-issue required commercial and shipping documents.

Failure to transfer risks via insurance/errors in insurance coverage

If the appropriate insurance coverage is not maintained for some reason, the importer will be exposed to financial losses stemming from cargo damages during transportation. The failure to keep appropriate coverage for the cargo can be traced to a lack of knowledge to identify the risks involved or a lack of understanding of the terms and coverage included in the policies. Insurance coverage is an essential part of the risk mitigation strategies for goods transportation and storage. The importer should constantly monitor the level of coverage available for imports. For more information, please refer to Page 24, "The importance of insurance coverage" section.

Tip - Due to significant potential financial losses that might result from damages during transportation or storage, importers should carefully analyze the coverage specified in cargo insurance policies.

Cyber-attack risks

In recent years, global commerce witnessed a significant increase in cyber-attacks targeting companies that are part of domestic and international supply chains. The current trends of digitalization and automation aim to provide end-to-end visibility in global supply chains. However, these developments in digitalization and automation are also creating increased exposure to cybercrime in the supply chain industry.

As a cyber-attack can disrupt the supply chain's operational performance, companies should have in place sound cybersecurity programs. These programs require participation from all levels of the organization, recognizing that cybersecurity is no longer just an information technology issue.

The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce has developed a risk management framework companies can

apply when developing cybersecurity programs. Core activities within the cybersecurity framework highlight the importance of identifying critical assets and ways to protect them, continuously monitoring threats, and developing appropriate response measures and recovery actions.

Box 2: Cyberattack on Colonial Pipeline

In May 2021, a cyberattack forced Colonial Pipeline to take the pipeline system offline for six days. Colonial Pipeline operates approximately 5,500 miles of pipeline connecting refineries in the U. S. Gulf Coast to consumption points in the East Coast for transportation fuels and other refined products. The disruption halted fuel deliveries and created shortages, long lines at gas stations, and price increases in several states. This ransomware attack highlights the importance of protecting critical supply chains against cyber-risks.

As cyber-threats are constantly evolving, company-wide awareness and training should be the cornerstone of a successful cybersecurity program.

3. Preparing for the Unexpected in Supply Chain Operations

Supplier's evaluations

The best way to prepare for unexpected interruptions in the supply chain is to perform a complete evaluation of all suppliers, including cost, quality, reliability of products, capacity, technology, and willingness to share information. A standard method of selecting a supplier is to use a supplier scorecard, which provides a weighted average of all relevant selection criteria.

In the simplified scorecard example below, weights associated with the selection factors are applied to each supplier's score. The scores should reflect the different

aspects of the supplier's performance, which are linked to Key Performance Indicators (KPIs). After applying the same scorecard to both suppliers, the supplier with the highest weighted score is selected.

Factor	Weight (0-100%)	Supplier 1		Supplier 2	
		Score	Total	Score	Total
		(0-100)		(0-100)	
Cost	20	90	18	70	14
Responsiveness	20	60	12	60	12
Delivery	20	75	15	75	15
Quality	40	60	24	90	36
Total score	100		69		77

Table 1. Example – Supplier Selection by Supplier Scorecard

Evaluations of reshoring and near-shoring vs. offshoring

One of the most critical decisions for a company is whether to make or buy a particular product needed for its operations. When making this decision, companies need to consider different possibilities for this sourcing:

- a. Offshoring. This option typically refers to relocating production (manufacturing and services) activities to a different country. One of the main drivers for companies to offshore production of supplies is the lower cost of manufacturing and operations in the offshore location.
- b. Near-shoring. Near-shoring implies sourcing the particular supply from a country located closer to the domestic market. For example, near-shoring could involve a U.S. company evaluating the possibility of changing the source of input from China to Mexico or Central America, closer to the U.S. domestic market.

-
-
- c. Reshoring. Reshoring implies the return of production activities previously offshored to in-house manufacturing or a domestic market manufacturer.

When evaluating offshoring decisions, the product or service's total cost must be evaluated. While wages may be lower overseas, the firm should consider other factors, such as supplier productivity, transportation costs, and U.S. import tariffs. Other qualitative factors must also be considered, such as potential exchange rate fluctuations, intellectual property risks, political disruptions, future cost trends, transportation risks, and quality issues.

Monitoring documentation, terms of trade, and terms of payment

The final cost of imported goods is easier to control when all relevant documentation is actively monitored throughout the transaction and shipment. It is crucial to review in detail the terms of trade and the terms of payment. Here are some best practices:

- a. Knowing and understanding the incoterm of a shipment is one of the best ways to control the risk associated with international transportation.
- b. All invoices and purchase orders must clearly state the incoterm applicable to the particular shipment.
- c. If utilizing a letter of credit in a transaction, it is important to review and ensure the accuracy of all commercial documents involved in the transaction, as amendments to letters of credit are costly.

The importance of insurance coverage

Cargo insurance is one of the primary mechanisms to obtain protection against potential losses during the transportation or storage of goods. The insurance will transfer specific importer's risks to the insurance company in exchange for a fee or a premium. The unexpected can happen and does happen. Hence, it is essential that the importer reviews and verifies the insurance level required for the cargo. Often importers do not have a clear picture of how the liability works in the event of a cargo loss. A freight forwarder or an insurance broker can help verify the insurance levels and advise the appropriate coverage for the specific type of cargo and transportation mode.

In many cases, the importer might not be aware that the insurance required by the cargo could be well above the basic coverage offered. For example, the insurance required by the CIF (Cost, Insurance and Freight) incoterm is just the basic coverage available (Coverage C under Institute Marine Cargo Clauses policies). For many containerized goods, the insurance required to fully cover the cargo's value is well above this basic coverage. To avoid potential losses, the importer should check that appropriate insurance coverage based on the value of the cargo.

Another common mistake is overlooking exclusions to the freight cargo insurance policy, such as improper packing. For example, if the supplier does not provide the appropriate packing for the goods and these get damaged during the transportation, this would be an automatic exclusion from the cargo insurance policy. The carrier would not be liable for the damages. Even for the "all-risks" policies, the importer needs to verify in detail the risks that are excluded from the policy and take the appropriate mitigation strategies. Additionally, the importer should always verify that the marine insurance cargo policy includes coverage for the general average risk (See more details in Box 3).

As importers rely more on complex, long supply chains, a significant disruption can result in a partial or complete operational shutdown. Many importers do not have

a clear picture of the real cost of a disruption in their operations without proper coverage. Besides having a comprehensive risk management program in place, importers can consider specialty insurance policies such as Contingent Business Interruption (CBI) and supply chain coverage. The objective of these policies is to offer protection against lost profits and disruption costs. The CBI coverage typically provides protection if a supplier's disruption is caused by physical property damage.³ The supply chain coverage is broader than the CBI. An insurance specialist can provide valuable help in determining the risks that can be covered under a CBI or a supply chain coverage.

Furthermore, the growing number of cyber-attacks makes cyber insurance a new area of interest for importers. A cyber-attack can also create significant disruptions in supply chains. For example, one potential disruption occurs when suppliers or carriers are unable to deliver the goods due to a cyber-attack in their IT systems. The importer should analyze potential coverage for this type of event with an insurance specialist.

³ Insurance Information Institute. Do I need business interruption insurance? June 15, 2020. Retrieved from <https://www.iii.org/article/do-i-need-business-interruption-insurance>.

Box 3: General Average and the M/V Ever Given

There are concepts in maritime insurance that are unique to this industry. A commonly used concept in ocean transportation is “general average” or general loss. If there is a loss during a voyage as a consequence of efforts to save the vessel (i.e., jettison, fire, stranded or grounded vessel, etc.), the damage losses are shared by the owner of the ship and all the cargo owners in the same vessel. Note that this includes the owners of cargo that was not damaged. For example, if there was a fire in part of the vessel, the cost of the fire damage will be shared by the owner of the vessel and all the cargo owners in that vessel, even those whose cargo was not affected by the fire.

In the more recent case of the M/V Ever Given, the vessel ran aground at kilometer 151 of the Suez Canal, blocking the vital waterway for six days, creating a massive disruption to international maritime supply chains. The queue reached 367 vessels just before the M/V Ever Given was successfully refloated. The owner of the vessel declared general average. This declaration implies the cargo owner’s obligation to contribute to any loss before containers can be released.

The situation of the M/V Ever Given highlights the importance of having the appropriate cargo insurance coverage. The liability stemming from general average declarations makes cargo insurance a wise decision for importers.

4. Supply Chain Disruptions

Major disruptions, such as the tsunami and nuclear disaster in Fukushima, Japan, and the COVID-19 pandemic, have made the logistics industry revisit the necessary level of preparedness and the level of resilience of critical operations during these external risk incidences. The ongoing events and repercussions of the COVID-19 pandemic have stress-tested domestic and global supply chains. The global impact across countries and value chains has been heterogeneous.

Understanding potential disruptions and their ripple effects is paramount to raising the preparedness level.

Types of disruptions

Among the different types of risks, external risks are frequently associated with disruptions to the supply chain performance. External risks include fire, natural catastrophes (earthquakes, volcanic eruptions, floods, and others.), economic downturns (financial crises), human-made disasters, terrorism and piracy, strikes, pandemics, and cybersecurity attacks. All these potential disruptions can severely affect the performance of critical parts of the supply chain. A common feature of these disruptions is the low probability of occurrence and a very high impact.

Disruption effects

Disruptions could create long-term impacts on the critical performance of the supply chain. For example, COVID-19 brought the need for a contactless supply chain into focus and accelerated current digitalization trends in the supply chain industry. This change will be the "new normal."

The digital transformation in supply chains seeks to achieve greater operational efficiencies and asset utilization. Current trends in supply chain digitalization include rapid developments in automation, increased reliance on Internet of Things (IoT) technologies and Artificial Intelligence (AI), the potential for 5G communications, advancements in autonomous systems, and digital supply chain twins, among others. One of the main aims is to reach complete supply chain visibility by implementing greater information exchange and integration among supply chain partners. The main risk of digitalization lies in greater exposure to cyber-risks and disruptions associated with cyberattacks. Hence, digitalization needs to be complemented by enhanced cybersecurity measures along the whole supply chain.

The propagation of the disruption through the supply chain is called the "ripple effect." The magnitude of this ripple effect is increased by the following factors: the practice of single sourcing, low safety stocks for complex supply chains, unclear criteria

for stockpiles, suppliers at 100% capacity, and a lack of contingency plans. On the other hand, the ripple effect is reduced or contained by redundancies along the supply chain, the speed, and the magnitude of the mitigation measures.

Tip - The first step in preparing for disruptions is to identify supply chain vulnerabilities. A company cannot get prepared for something it is entirely unaware of. Prepare a *risk register*. This register should contain all relevant external risks for the supply chain, their expected likelihood, and their impact.

Mitigation strategies for disruptions

Companies need to consider the potential mitigation strategies for each of the identified vulnerabilities. Companies should devote efforts to determining specific mitigation/response actions to be taken once the disruption affects critical performance and the ripple effects are spreading through the chain.

In terms of mitigation strategies, the following redundancies and flexibilities should be considered:

- a. Flexible supply base with backup suppliers and supply chain diversification. A more flexible supply base and a diversified supply chain will provide better insurance than single sourcing. Diversification is also important to reduce the company's risk of relying on one supplier.
- b. Surge manufacturing capacity. Consider an agile manufacturing base that can provide incentives for flexible production lines, which can be re-programmed/retooled in case of need (i.e., repurposing factory production). For example, during COVID-19, several factories were repurposed to produce essential medical supplies.
- c. Shortening supply chains or near-shoring/reshoring. One way to reduce the risk associated with long and complex supply chains is to reduce the length of supply chains. In this respect, U.S. companies could consider

near-shoring or reshoring from Asia. Instead of having the supplier in China or South Korea, the company switches to a closer supplier in Mexico or Brazil. Reshoring happens when the manufacturing process is relocated back to the U.S. market. The manufacturing postponement, or the action of delaying the customization of standard units until they reach their destination market, provides one way of bringing back some offshore activities to the domestic consumption market. Also, a reduction in the number of intermediaries will shorten the supply chain.

- d. Stockpiles and safety stock. The computation of safety stocks for different supply chain items needs to be adjusted and the expected vulnerabilities - included in the risk register. Besides, reviewing the existing criteria for managing stockpiles, including shelf-life issues, is essential. An additional advantage of the stockpiles may be reflected in creating a long-term demand to keep surge manufacturing contracts.
- e. Adoption of new technologies for managing complex chains. Better data analytics and the adoption of Artificial Intelligence (AI) will enhance the capabilities to manage complex and dispersed supply chains, improving the ability to handle disruptions in long, international value chains.⁴
- f. Supply chain partner collaboration and communication for finding alternate sources in crisis times. To manage the response to a disruption, all supply chain partners will benefit from a *control tower* approach. In this approach, a centralized system for all information will provide essential visibility for decision-making during disruptions. Full collaboration with suppliers and customers in developing recovery and continuity plans will be vital in deploying an adequate response.

⁴ For additional details, see The Impact of Artificial Intelligence on International Trade, J. Meltzer, Brookings Institution report, December 2018

-
-
- g. Development of contingency plans and business continuity plans. The fastest response to disruption will come from companies that prepared well in advance with contingency and business continuity plans. Pre-determining all partners' roles and responsibilities is one of the best responses against disruptions.

The more capabilities are built into the supply chain, the smaller the ripple effect will be and the faster the recovery time in terms of operational performance.

Tip - The management of the supplies for the importing process requires preparedness. This implies having plans well in advance of any significant event that might disrupt the supplies for the importing operation. The key for preparedness is to have well-defined roles and responsibilities in case of a disruption.

Resilience monitoring

Risks are constantly changing and evolving, and companies should periodically monitor different supply chain risks to be prepared. Companies would benefit from establishing a risk management system to monitor the evolution of different vulnerabilities. Periodically update the risk register and reassess the probability and impact of future disruptions, as well as the planned mitigations.

A control tower approach will monitor the flexibility and redundancy in the supply chain in addition to the risk management system. For this monitoring, a company should not just map its first-tier suppliers but also its second-tier suppliers. This visualization will help to anticipate potential ripple effects throughout the supply chain (See Figure 6).

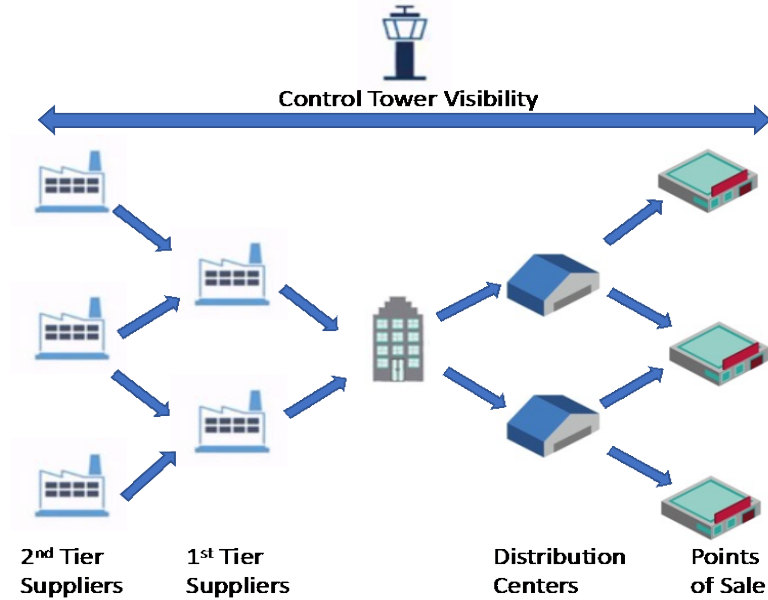


Figure 6. Control Tower Visibility

Tip - The risk register should be reviewed every year. Vulnerabilities change over time. A company may face new risks or different versions of old risks. Add the mitigation strategies in the risk register, too. Business owners can review periodically if the proposed mitigation is still the best option available.

FINAL THOUGHTS

The pandemic unveiled the complexities of international supply chains and how they could be subject to substantial disruptions, bringing the concept of resilience to the forefront of supply chain planning. The previous sections provided an overview of the most common supply chain risks and their impacts, as well as mitigation strategies for disruptions in the logistics process. The recommendations of this white paper are

intended to serve as good practices for importers and supply chain, transportation, and sourcing professionals. Key takeaways include:

- Companies must allocate time and effort to assess if their current supply chain strategies will be able to cope with short- or long-term disruptions.
- The importer should identify the main supply chain vulnerabilities and establish a risk system to monitor their evolution.
- The importer must review the exposure to the most common supply chain risks. The following questions can help importers to assess potential exposures:
 - Are you relying on single source suppliers?
 - Do you have a clear map of your supply chains, including locations?
 - Do you know your supplier's supplier?
 - Do you constantly monitor if the appropriate insurance coverage is maintained?
 - How sound are your cybersecurity measures?
- When evaluating offshoring decisions, the product or service's total cost must be evaluated together with other relevant qualitative factors such as quality, responsiveness, flexibility, etc.
- One of the best ways to prepare for the unexpected is to perform a complete evaluation of all suppliers.
- Importers should carefully analyze the coverage specified in cargo insurance policies. A freight forwarder or an insurance broker can help verify the insurance levels and advise the appropriate coverage for the specific type of cargo and transportation mode.
- The supply chain should have redundancies or mitigations proportional to the anticipated vulnerabilities to disruptions.

-
- It is essential for importers to have contingency plans or business continuity plans in place. The key for preparedness is to have well-defined roles and responsibilities in case of a disruption.
 - Keep a risk register and monitor the different risks in terms of their likelihood, their impact, and potential mitigations. Importers should review periodically if the proposed mitigations are still the best options.

We encourage importers to go beyond these good basic practices and explore the resources detailed in the next section.

ADDITIONAL RESOURCES

This section provides some additional resources regarding the management of supply chain risk and maintaining business continuity.

1. [Supply Chain Risk Management Practices for Federal Information Systems and Organizations](#), NIST, U.S. Department of Commerce,
2. [Cybersecurity Framework](#), NIST, U.S. Department of Commerce,
3. [Supply Chain Risk Management: Reducing Threats to key U.S. Supply Chains](#), National Counterintelligence and Security Center.
4. [What is Business Continuity? \(video\)](#) The Business Continuity Institute,
5. [Incoterms 2020/ Incoterms 2010](#). International Chamber of Commerce
6. Resources for Foreign Exchange Hedging
 - a. [GPS Capital Markets](#)
 - b. [Bannockburn Global Forex](#)
7. [Insurance Information Institute](#).
8. [The Power of Coherence](#). P. Leinwand and C. Mainardi, Harvard Business Review, June 2010.
9. [The Impact of Artificial Intelligence on International Trade](#). J. Meltzer, Brookings Institution, December 2018.