Supply Chain Risk

Supplier failure can severely impact operations. Assessing the vulnerability of suppliers is an essential part of business continuity.

Original Issue: September 2012 Subscribe to Preparedness Bulletins Reissued 2021

Covid-19 has significantly impacted the global supply chain, and experts forecast disruption will continue for an extended period. It's not the only cause or contributing factor affecting global commerce. Demand for goods spiked as Covid shutdown factories. Inadequate capacity to off-load ships and transport goods has contributed to delays.

Amid the pandemic, flooding in China and Europe heavily damaged communities, disrupted manufacturers, and affected rail links. Cyber-at-

Port Newark Container Terminal
Photo by Preparedness, LLC

tacks on the Colonial Pipeline and the world's largest meat supplier disrupted supplies.

Disasters around the world have and will continue to disrupt the global supply chain. Hurricanes continue to impact the continental United States from the Gulf of Mexico to the Northeast. Catastrophic wildfires in the western United States affected wide areas of the Pacific Northwest. Covid-19 isn't the only pandemic to impact global commerce. SARS in 2004 and Swine Flu in 2009 impacted travel and raised fear around the globe.

Natural disasters are a frequent cause of supplier failure, but transportation disruptions, cyber-attacks, and geopolitical events have exacted a toll as well. Political tensions in multiple regions of the world are an ever-present concern.

The cost of a supply chain interruption can be significant. A lightning-caused fire within a clean room at a Philips Electronics chip-manufacturing plant in Albuquerque, NM was extinguished in 10 minutes. At the time of the March 17, 2000, fire, Philips was a supplier of radio frequency chips to Nokia and Ericcson. Nokia's aggressive action following the fire enabled them to overcome the interruption in their supply of chips. Ericcson had no "Plan B" and withdrew from the handset market. Insurance didn't fully cover their losses, and Ericcson reported a $256 million pre-tax loss at its handset unit[1].

Decades of effort to maximize efficiency and value in the supply chain, "offshoring" production, and "just in time" delivery systems have created significant vulnerabilities.

Causes of Supply Chain Interruption

A supply chain can be impacted by:

- Physical damage to a supplier's facilities or supporting infrastructure
- Damage to or failure of critical production machinery, equipment, and or control systems
- Failure of a supplier's supply chain

1 Dow Jones News Service, July 21, 2000

- Strike or job action
- Interruption or disruption of transportation and logistics from the suppliers to customers
- Failure of communications with supplier including electronic data interchange
- Supplier bankruptcy
- Supplier consolidation
- Geopolitical events

Business Impact Analysis Identifies Critical Supplies

Analysis of supplier risk should begin by focusing on the products that generate the most value to the organization. "Value" can be defined by revenue, margin, growth potential, or other factors.

Conduct a business impact analysis (BIA)—part of the process of developing a business continuity plan—to identify the potential operational and financial impacts from supplier failure. For more information on conducting a BIA, review the Preparedness Bulletin "Business Impact Analysis."

Products and services that generate the most value to the organization should be priorities for supplier risk analysis. Identify the raw materials, parts, sub-assemblies, components, and services that go into the manufacture of products that generate the most value. Compile a list of the suppliers and service providers by product line. Sort the list by contribution to overall value to your organization. If you have a long list of suppliers, those at the top of the list should be priorities for risk analysis.

Determine which suppliers and service providers are sole and single source. Sole source suppliers and service providers have no alternate. If they fail, the dependent product cannot be manufactured. Alternates may be available for single source suppliers, but it may take considerable time to qualify an alternate to meet quality, regulatory, or contractual requirements. Cost is often an issue when switching suppliers but may not be the primary consideration.

Compile a list of suppliers that includes supplier name; materials provided; classification (single, sole, or multiple source); total amount of money paid to the supplier each year (this "spend" helps to determine the leverage you may have with the supplier); and most importantly from the BIA, the potential revenue lost if the supplier were to fail. Include a column for a "risk score" to be developed when you survey your suppliers. Sort the list with the suppliers that could cause the greatest revenue loss at the top of the list.

Suppliers at the top of the list that are classified as sole source would be the top priority for further assessment. Single source suppliers at the top of the list also deserve scrutiny if the inventory on hand would be exhausted before you are able to find and qualify an alternate supplier. Evaluate the number of days that a minimum inventory level would hedge against any delays in receiving from sole and single source suppliers.

Assessing Supplier Risk

Conduct a survey of your suppliers to assess their resiliency and the likelihood that they could fail to meet your supply requirements. Resiliency is a measure of the supplier's ability to withstand and recover from any interruption or disruption of their manufacturing or distributions operations. Surveys can be done in various ways.

Online tools are best when surveying large numbers of suppliers. Each supplier logs into a secure website, answers questions, and attaches requested documents. Online surveys can be automatically scored, and survey information can be exported into a spreadsheet or database for analysis. Surveys can also be conducted via electronic mail, over the telephone, and in person.

Constructing a Supplier Risk Survey

Surveys should gather information required to assess the risk of supplier failure. Carefully crafted questions with supporting instructions will ease survey completion and enhance response accuracy. Emphasize that survey completion requires the input of technical experts within the supplier's organization. Sales or customer relationship managers usually do not have knowledge of building construction, hazards, protection, business continuity programs, and the supplier's financials to answer all questions.

The supplier risk survey should capture the following information:

- Facility description
- Hazards and other risks

- Loss prevention and risk mitigation efforts
- Supply chain risks
- Emergency response, business continuity, and IT disaster recovery plans
- Certifications
- Financials

Facility description. The survey should ask for the locations of manufacturing and distribution facilities that supply your organization. This information enables assessment of regional hazards including natural hazards and political risk. Addresses can be used for computer modeling and aggregating the risk of multiple suppliers in the same area. Construction information (e.g., age, type of construction, firewalls, etc.) paints a picture of the resiliency of the building.

Hazards & Risks. Questions regarding whether facilities are in flood zones, earthquake zones, or in proximity to the coast (i.e., exposed to tropical cyclones) should be included. Questions regarding the storage and use of significant quantities of hazardous materials (dangerous goods) including ignitable liquids and flammable gases identify a facility with greater potential for a catastrophic fire or explosion.

Loss Prevention & Risk Mitigation. Determine whether a supplier's buildings are equipped with automatic fire detection and suppression systems and intrusion alarm systems. Facilities that have fulltime personnel responsible for safety and security are typically safer than those without qualified personnel managing risk. Determine whether security guards provide surveillance. Ask questions about risk assessment activities and the scope of health, safety, and fire prevention programs. Question whether critical machinery and equipment undergoes preventive maintenance and spare parts are on hand.

Supplier's Supply Chain (Your Tier 2 and 3 Suppliers). A risk to your supplier's supply chain could also be a risk to you. If a supplier has critical sole and single source suppliers, then the supplier's operations may be at greater risk. Suppliers with raw materials or parts with long lead times pose greater risk because of the longer time to replace raw materials and parts. Verify that your suppliers have required licenses for the software and intellectual property that goes into the components that they supply to you.

Business Continuity Programs. For years, companies have been asking their suppliers whether they have a business continuity program. "Yes" was the quick answer, and no further investigation was undertaken. Now that more industries are required to have business continuity programs (e.g., financial services, government contractors, etc.), the question has been replaced with a detailed questionnaire sometimes followed by an on-site audit.

A detailed set of questions should be designed to determine whether there are standards-compliant programs in place. Questions should ask whether there is an emergency response plan, business continuity plan, and information technology disaster recovery plan.

Investigate the resiliency of systems supporting electronic data interchange with time-sensitive suppliers.

These plans should be based on an assessment of risks to the facility and business processes. Roles and responsibilities should be clearly defined for foreseeable threats; continuity and recovery strategies should be described in detail; resources required to execute strategies should be identified; strategies should be tested; personnel should be trained; and plans should be exercised periodically.

Certifications. Companies that have been certified to international business continuity, quality, environmental management, and other standards have demonstrated a commitment to managing risk. The survey should ask what standards the facility is certified to and the period when the certification is valid.

Financials. Assessing a supplier's financial situation is also important. Asking questions about ratings, revenue growth, debt to equity ratio, potential legal judgments (against them), and collective bargaining agreements about to expire can help you assess the financial condition of your supplier.

Documentation

Throughout the survey include requests for documentation including facility and site plans, risk assessments, emergency response, business continuity, and IT disaster recovery plans. Site plans provide a picture of production and distribution facilities; their separation; and their proximity to

hazards. A review of program documents will provide insight into the thoroughness of a supplier's planning and their ability to respond to business disruptions. If suppliers won't provide copies of their plans, ask for a copy of the title page and table of contents. These pages will enable you to determine when plans were last updated and gain insight into the depth of planning.

Scoring The Surveys

Online risk surveys can be programmed to generate scores based on the weighting of the questions and answers. All questions are not equally important, so carefully weight each section, question, and answer.

Keep in mind that the overall "score" is only good for comparing surveys from suppliers that have completed the same survey.

Evaluating The Surveys

Evaluating survey results involves much more than looking at the raw score. Call upon your technical specialists to help you interpret the results and assess the documents that were submitted along with the survey. Review the answers to the questions looking for blank or incomplete answers, inconsistencies, and answers that don't seem right. Confer with suppliers if to clarify any questions. Adjust the score to reflect positive and negative information.

Next Steps

Look closely at your list of critical suppliers—those that could cause the greatest financial impact to you should they fail. If they score poorly on the supplier risk survey, then you may want to dispatch your experts to conduct an on-site evaluation of the supplier.

Identify and qualify alternate suppliers for critical single source suppliers. Alternates should not be subject to the same regional events as your primary supplier. Investigate product redesign, inventory management, and other strategies to hedge against sole source supplier failure.

Risk management should utilize the financial loss estimates gleaned from the business impact analysis to determine whether to purchase contingent business interruption insurance coverage (CBI) and if so, limits of coverage to purchase.

Loss prevention, hazard mitigation, and preparedness programs should always be pursued—even for suppliers that score well.

About Preparedness, LLC

Preparedness, LLC is a client-focused risk consulting company. Our mission is to safeguard people, protect property, minimize business interruption, and protect an entity's image and reputation. Our vision is to thoroughly understand each client's business and become a long-term, trusted advisor.

If you have questions, or need assistance with the development, implementation, or evaluation of your preparedness program, please contact us.

Subscribe to Preparedness Bulletins

Click here and sign up for our Preparedness Bulletins. You can unsubscribe at any time.

PREPAREDNESS, LLC

(781) 784-0672

INFO@PREPAREDNESSLLC.COM

HTTPS://PREPAREDNESSLLC.COM