To The Point
Supply Chain Risk Management

CHUBB®

Overview

In today's manufacturing industry, there is a growing tendency for corporations to outsource key manufacturing processes. The main reasons for outsourcing include:

- Cost control
- Flexibility
- Increasing complexity and specialization
- Ever-increasing focus on marketing and sales

The globalization of business and the manufacturing industry have made it imperative for executives and risk managers to reassess how they manage the growing number of risks facing their organizations. This is especially true for risks impacted by supply chain interruptions. As economy and business practices have changed, vendors and suppliers have become more intertwined with an organization's ability to respond to disasters.

Outsourcing, offshoring, and lean manufacturing may help to streamline a production process but can also jeopardize the resiliency of the supply chain. New risk factors have developed from a pressure to enhance productivity, eliminate waste, remove supply-chain redundancy and drive down cost.

In considering the resilience of a supply chain, the complexity of risk is commonly underestimated. Although many companies tend to focus on dealing with internal (process) risks, supply-chain disruptions can also arise from external sources such as a fire at the premises of a critical supplier or from natural disasters. Significant supply-chain disruptions can reduce a company's revenue, cut into market share, inflate costs, and threaten production and distribution.

Revenues at Risk

The supply chain is subject to a myriad of factors that can result in a disruption. A few examples of these factors include:

- Political risk
- Labor strikes
- Weather and other natural catastrophes
- IT failures
- Bankruptcy

When developing a supply chain risk-management program, it is critical to focus on key suppliers.

Over the past years, incidents of flooding, earthquakes, and hurricanes have subjected thousands of firms to disruptions that have closed plants for days or weeks and directly resulted in billions of lost revenues. Some of these firms never recover or recover so slowly that the clients who rely on them are forced to find other suppliers or suffer significant loss of revenue themselves.

Supply-Chain Risk-Management Process

To manage supply-chain risks, the following should be considered:

- Senior management must acknowledge that there is an exposure and a risk associated with the supply chain. Only then will the issue get prioritized and funded.
- A comprehensive Business Continuity Plan should anticipate surviving supply chain interruption and continually engage senior management and supply chain managers.
- Mapping the supply network - this entails building a structure of the various participants in the supply chain. These are typically third-party manufacturers or subcontractors, warehouses, and distribution centers but could also include transport and shipping partners.

Once your suppliers have been identified, legal counsel should review contracts to determine if the proper protections are in place for your organization. They should also determine each party's responsibilities in the event of a supply chain interruption. Contracts should require that your suppliers have business continuity plans in place to address their own supply chain impairments. Just as your organization wants to be prepared, you want your suppliers to be prepared as well.

Identify and Assess the Risk

Assessing the supply chain risk relies on the engagement of the business continuity team. This involves building a cross-functional team of subject-matter experts. The team defines enterprise risk relating to financial, strategic, hazard, and operational areas.

This process should include vendor questionnaires followed by on-site assessments of vendor operations, warehousing, and other critical elements of the supply chain. Spot checks should be regularly performed to assure suppliers are adhering to sound business continuity risk management practices.

The depth of the supply chain should also be addressed since redundancies may be false. For example, your Tier 1 single-source supplier may not have any supplier redundancies for their Tier 1 suppliers. Many supply chain losses are caused by "sub-tier" suppliers, and businesses tend to underestimate the length and frequency of the disruptions.

Key Suppliers

When developing a supply chain risk-management program, it is critical to focus on key suppliers. Key suppliers are defined as those which have the potential to cause a significant business interruption loss to their clients' companies by a single incident such as fire, explosion, flood, or earthquake.

Key suppliers have several characteristics in common. Among the most important are:

- A high amount of value added by the client is dependent on the supplied products.
- Supply is dependent on a single production site or even a single production line.
- Limited possibilities to transfer production to other sites.
- Long lead times that can delay recovery or find alternative suppliers/ production.
- Production has been shifted to a third-party supplier where unique production machinery is required.

These suppliers should have the most stringent business continuity requirements to continue to do business with your organization, as their emergency incidents may quickly become yours without adequate preparation.

Business Interruption Considerations

Business continuity planning is fundamental to improved supplier/vendor resiliency. Key suppliers should have their own formal business continuity plan in place since it will generally reduce downtime following a major disruption.

Devising and implementing a business continuity plan for the supply chain is not a simple process. To protect your organization, you must first understand what makes it vulnerable. A Business Impact Analysis (BIA) identifies and ranks the types of events or hazards that are most likely to threaten your business. Examples of categories addressed within this assessment, in addition to supply chain, include:

- Facility construction
- Fire protection
- Specialized equipment
- Natural disaster potential
- Utility susceptibility and redundancy
- Staffing
- Technology resources
- Security
- Past events

By determining the likelihood, potential impact, and current resources related to disasters, the extent of vulnerability can be assessed. Immediate steps may be available to significantly reduce vulnerabilities. Two examples include maintaining safety stock and having numerous pre-qualified suppliers/subcontractors:

- Safety stock involves having an inventory of materials on hand to allow for a temporary loss of supply from the vendor. This an effective means of reducing the exposure from the loss of a single-source supplier for a short-lived disruption, especially for those companies operating on a just-in-time production schedule.
- Secondary supplier qualification should be an ongoing process designed to reduce the impact from the loss of a single or sole supplier. It is a common misconception that secondary suppliers will be readily available, and firms are far too optimistic on the time required for a secondary supplier to ramp up production while maintaining quality standards. Just as your organization will be seeking to source secondary suppliers in an emergency, so will your competitors.

Conclusion

Making supplier networks more secure is expected to become a higher, if not the highest, priority for the risk management community. This is especially true as businesses continue to rely on outside suppliers, both foreign and domestic, to supply services and materials that might have been handled in-house in the past.

Learn More & Connect

For more information on protecting your business, contact your local risk engineer, visit the Chubb Risk Consulting Library, or check out www.chubb.com/engineering.

Chubb. Insured.℠

Form 09-10-0976 (Ed. 4/21)

CHUBB®

Supplier/Vendor Questionnaire

Class Description	Yes	No	N/A	Action Needed
1. Does your company have continuity plans in place that includes top management, a thorough risk assessment, and regular testing and review to ensure its effectiveness?	☐	☐	☐	
2. Do plans include the recovery of both business functions as well as IT applications?	☐	☐	☐	
3. Is there any third-party verification of the plan's effectiveness?	☐	☐	☐	
4. Who is responsible for the business continuity planning in the organization?	☐	☐	☐	
5. Do you rely on any single source suppliers?	☐	☐	☐	
6. How long would it take to replace these suppliers?	☐	☐	☐	
7. Do you have backup suppliers pre-qualified?	☐	☐	☐	
8. Are there contingency plans to run production machinery with reduced staff, if full staffing is not possible temporarily?	☐	☐	☐	
9. Are there multiple geographic locations that would allow for production/work to be moved to an unaffected/less affected location?	☐	☐	☐	
10. Are there production equipment redundancies at multiple locations, or do you have backup suppliers that can be used in the event of a work-stoppage event?	☐	☐	☐	
11. Do you have excess product stored at offsite locations such that you can continue to distribute product?	☐	☐	☐	
12. Do you have multiple product transportation providers, or multiple locations where your own vehicles are located, so you can continue to transport goods?	☐	☐	☐	
13. Has a business impact analysis been completed to identify critical business/IT functions and the associated recovery time objectives?	☐	☐	☐	
14. Is there a cybersecurity plan in place, and do you have a robust testing and continual upgrade plan in place to prevent cyber intrusion, hacking, or the compromise of sensitive data?	☐	☐	☐	
15. Are there trained emergency response teams around the key exposures that would impact operations, such as fire, earthquake, hurricane, or tsunami?	☐	☐	☐	
16. Are there prearranged agreements with disaster restoration companies to move you to the "front of the line" in the event of a widespread emergency event? Does this include access to generators and water pumping equipment?	☐	☐	☐	
17. Have recovery strategies been developed to meet established recovery time objectives?	☐	☐	☐	
18. Has your company established a crisis communications plan?	☐	☐	☐	
19. Does the plan include provisions for pandemics?	☐	☐	☐	
20. Are the plans reviewed and tested at least annually?	☐	☐	☐	

Chubb. Insured.℠

Form 09-10-0977 (Ed. 4/21)