National Institute of Standards and Technology
U.S. Department of Commerce

U.S. Resilience Project

BEST PRACTICES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Communications Company
One Company's Supply Chain Transformation Journey

INTERVIEWS

Senior Manager
Supply Chain Operations Strategy

Manager
Procurement Strategy

The Next New Thing in Supply Chain Risk Management

Testing the Business Continuity Plan (BCP): Recently this high-tech communications company raised the bar on business continuity requirements by requiring one of its top ten suppliers to conduct a full-scale, real-time simulation to prove that it can recover within the timelines committed to in their BCP.

Company Overview

Approximately four years ago, the company went through a major reorganization and divestiture. Now a $6 billion dollar critical communications technology company, it serves a global marketplace with more than 50,000 customers in more than 100 countries, ranging from public sector customers at local, state and national levels to small businesses to Fortune 500 companies. Its core markets are in public safety government agencies, retail and hospitality, manufacturing and field mobility, transportation and logistics, energy and utilities, and education and health care.

The reorganization left the company with some serious supply chain challenges — an array of legacy systems, outdated Enterprise Resource Planning (ERP) systems, a supply chain that was ill-suited to a customer-driven focus. In a fiercely competitive global marketplace, it had to improve on-time delivery, reduce lead times and critical parts shortages, and reduce inventory and carrying costs.

Figure 1. Post-Reorganization Goals

Initial State	Desired State
Regional/Site Focus	Global Processes
Perfect the Pieces	Company-wide Improvements
Reactive	Proactive and Ready
Multiple ERPs	One ERP
Disparate Home Grown Tools	Integrated Cloud Application

Transformation through Collaborative Execution

One of the biggest challenges was that the company lacked the tight connections with trading partners that were essential to an efficient, fully functioning supply chain. The goal was to create end-to-end visibility among its supplier network and real-time collaboration across multiple tiers of the supply chain. It calls this concept "collaborative execution." The company defines collaborative execution as "...the ability of all partners in a global trading network to work together to resolve real and potential problems with the best available information — quickly, iteratively and cost-effectively."

To improve operational effectiveness, the company created a cloud-based platform to facilitate collaboration across a number of key supply chain processes — automated forecast and commit capabilities, automated inventory management, quality tracking process — that also strengthens supply chain continuity, security and quality as well. To implement supply chain change gradually, the company developed a phased implementation plan:

Figure 2. Managing Change Gradually

	Phase 1	Phase 2	Phase 3	Phase 4 (End State)
Roadmap	Capability Roadmap	Foundational Deployment	Global Onboarding	Process Maturity
People	Process Owners Change Leaders	Supervise Development	All Process Practitioners	Collaboration Innovation
Processes	Load and Chase	Plan & Execute	Anticipate & Shape	Delight and Disrupt
Systems	Architect the Solution	Implement Core Value Chain Planning Application	Complete Value Chain Planning Footprint	Fine Tune Applications

Strategic supply chain transformation is continuing. One of the next supply chain transformations: the ability to link pricing and supply chain — and change the pricing based on when the customer wants delivery. Supply chain executives contend that too much time and money is spent on making sure inventory is on the shelf, even though the company knows that a portion of its customers do not need it that fast. The company is investing in ways to make the supply chain across multiple tiers (supplier, manufacturer, and channel partner) more efficient in an effort create a win-win-win for all parties involved.

Organizational Approach to Risk

Even as the company was transforming its supply chain processes, it was taking a closer look at supply chain risk management — largely driven by supplier bankruptcies and natural disasters that had created supply chain chokepoints. It considers business continuity interruptions to be the primary supply chain risk — and is pro-actively addressing single points of failure and critical vulnerabilities.

A formal Enterprise Risk Management (ERM) program convenes twice a year to review the top 10 risks to the company and requires risk mitigation efforts for each. The company's experience over the years with supplier and component shortages means supply chain related risks regularly rank in the top 10.

Compared to other risks that result in a project based mitigation effort, there are dedicated Supply Chain Risk Management (SCRM) programs in place in multiple organizations in the company. First, the Supply Chain Transformation Team, focused on continuity and resiliency, is responsible for managing the end-to-end SCRM approach. In close partnership, the procurement team focuses on component and supplier risk and the product teams focus on product integrity and vendor security.

Business Case for Supply Chain Risk Management

Supply assurance to its customers is the primary driver behind its SCRM efforts. If its key products are not on the store shelves, customers will go to the competitors. Its known single points of failure are clear and shared by most other manufacturers:

- Single/Sole Source Components
- Joint Design and Manufacturing Partners (JDM/CM)
- Company owned facilities for in-house manufacturing

As new risks appear on the radar, new resources may be allocated to resiliency efforts. The corporate programs run very light on human resources and automated solutions. In part this is because the SCRM efforts have been successful to the point where risk mitigation is embedded in the daily operations. Many risk management best practices are considered simply "table stakes" for doing business.

Guiding Principles of SCRM

The principle focus of supply chain risk management is protecting revenue at risk — the company focuses on the top 80 percent of revenue. SCRM efforts are driven by a singular goal to ensure that 80 percent of the company's revenue target can be met with 13 weeks of a major disruption. In order to achieve the goal, the company uses a combination of three strategies:

- Migrating customers to a different tier product that may be available.
- Maintaining geographically diverse, and in some cases, redundant supply chain operations.
- Keeping sufficient inventory on hand to cover the time it would take to recover from a major event.

The revenue at risk metric is reported regularly to executive leadership as part of an Operations Executive Dashboard.

Practical Applications of SCRM

The SCRM program focuses primarily on vendor and continuity risks for both in house and contract manufacturing. Many requirements are baked into the supplier contracts, and the company holds the same standards for its internal operations. For example, both in-sourced and out-sourced factories are required to have reviewed and approved Business Continuity and Crisis Management Plans, as well as exercise their plans regularly. After the 2011 Japan earthquake, contract language was added to the pre-existing Business Continuity section requiring suppliers to communicate any crisis within a certain time frame. More recently, the company tightened scrutiny of one of its vendors by requiring them not only to have a BCP in place, but also to conduct a full-scale, real-time simulation to prove that it can recover within the goals stated in the plan.

Prioritizing Risks: Procurement manages component and vendor risks. For components, this is done through a very robust initial and continual assessment program.

Figure 3. Risk Matrix

Header	Header	Header	Header
Multi Source Component	1	More than 1 supplier qualified Primarily hardware, electrical passive components	Can take action at the time of the event
Single Source Industry Standard	2	Only 1 supplier qualified but other suppliers make a "drop-in" replacement part Should be able to dual source Primarily non-semiconductor electrical components or COTs part available from one or more suppliers	Can take action at the time of the event
Single Source Non-Industry Standard or Custom (Low)	3	Only 1 supplier qualified but other suppliers could replacement part Low effort (less than 3 months) to qualify alternate part Can be any customer electrical or mechanical part May require minor design changes Non-standard part, limited or no availability in distribution	Can take action at the time of the event
Single Source Non-Industry Standard or Custom (High)	4	Only 1 supplier qualified Other suppliers make alternate part but would take more than three months to qualify alternate Can be any custom electrical or mechanical part May require design changes Non-standard part, limited or no availability in distribution	Take action prior to the event
Sole-Source (High)	5	Only 1 supplier qualified with no other supplier able to make alternate part Unique technology process Major product redesign required to use part from alternate supplier No availability in distribution	Take action prior to the event

Each component is rated on a scale of one to five, where one is readily available from many suppliers and five is custom part with up to a year lead-time to replace. Components rated three, four or five must have a mitigation strategy in place, such as holding inventory or dual sourcing. Tier visibility varies depending on risk type, regulations and product line. Corporate Social Responsibility (CSR) regulations for conflict minerals require visibility to the lowest tiers possible.

Managing Vendor Risk: Due to the nature of their products, the company is very reliant on its vendor base. Many of the components do not have more than one supplier — and the cost of bringing on additional suppliers is significant. Consequently, the supply chain and procurement organizations routinely assess exposure, performance and compliance risks in its vendor network. At a high level, exposure risks including supplier financial health, input costs, legal risk and trade security. In contrast, performance risk considers site disruptions, cost pressures and long term alignment. Finally compliance risk takes into account CSR, ethics, environmental concerns and so on. The assessments are rolled up into a supplier financial health dashboard presented at the vice president level.

Different levels of suppliers undergo different levels of scrutiny. For example, the company does a financial health assessment for all tier one vendors, but will only drill into CSR issues for its long-term partners. Approximately 80 percent of their spend is with the strategically aligned key partners who undergo regular risk reviews. For their long-term suppliers, maintaining the relationship is just as important as the risk reviews and metrics. According to one procurement manager, "Its essentially a risk if you don't have that relationship when a problem arises."

Figure 4. Vendor Risk Management

Exposure Risk

Supplier financial health

Input costs (commodities, currency, labor)

Legal risk (intellectual property protection, terms and conditions)

Security (trade, counterfeiting, authenticity, supply chain security)

Performance Risk

Business continuity (natural disasters, geopolitical risks, supplier operations)

KPIs

- Quality
- Supply Assurance
- Delivery
- Long-term support and alignment from key partners

Compliance Risk

Corporate Responsibility (labor, health, safety)

Conflict Minerals

Ethics (code of conduct, Foreign Corrupt Practices Act)

Environmental (material restrictions)

Business Continuity Risks Supplier Rating and Audit: The company has developed detailed tools to audit its suppliers across a range of business interruption and recovery issues, including business interruption risk assessments, business impact analysis, business continuity planning, emergency transfer of operations, BCP testing and IT disaster recovery planning. The following is an example of the supplier rating system for business interruption and recovery risk assessment.

Figure 5. Supplier rating system

Level 1	Level 2	Level 3	Level 4	Level 5
No Risk Assessment Complete No policies or procedures for management review of risk assessment	Informal Risk Assessment Little evidence of employee awareness Recovery time identified to be 11-14 weeks	Well-defined procedure to characterize business interruption (BI) and recovery risks. Recovery time identified to be 7-10 weeks. Most areas of business have assessed risk and created mitigation plans Management has allocated resources to work on major risks.	Documented risk assessment system used by all major areas of business and periodically reviewed for improvement. Recovery time identified to be 3-6 weeks Change Control Board evaluates impacts on BI and recovery risks before changes are made Periodic reviews conducted with key customers Some employees trained in BI and recovery risk assessment procedures	Complete BI and Recovery Risk Assessment with internal audits Recovery time identified to be less than 2 weeks Customers are confident in and feel part of BI and recovery risk assessments. BI and recovery risk assessment program complements continuous improvement processes Al employees fully trained in BI and recovery risk assessment processes

Quality: The quality team resides in the supply chain organization and does regular assessments of its vendors:

- Supply Quality Management System
- Supplier Resource Management and Capacity Planning
- Production Process Quality
- Sub-tier Quality
- Quality Improvement
- Business Continuity Plans

Cyber risks: Given the nature of their products, supply chain cyber risks are not currently in scope for the SCRM program. Most of the software is proprietary, not open source, so risk is addressed in the product development process, not the supply chain. The supply chain focus is on compromised and/or counterfeit products. Purchasing directly from trusted manufacturers is a practice in the risk control process. In addition, the procurement, quality and product security groups focus on extensive product qualification, testing, secure purchasing practices and product tracking. It does employ a third party service to review potential counterfeit components during the product development phase and minimize the risk of introducing counterfeits into the production process.

Standards: In 2013, the company started to transition its suppliers to the new system used by members of the Electronics Industry Citizenship Coalition (EICC). EICC-ON evaluates supplier performance in the areas of labor, ethics, health, and safety and environmental sustainability. Supplier risk is rated from responses to self-assessment questionnaires at corporate and factory levels. High-risk suppliers are targeted for audits, and medium-risk suppliers are given feedback and invited to engage in dialogue to develop plans to address their risks.

Supplier self-assessments are backed by an audit program, in which detailed onsite audits are conducted by a third-party firm. The decision about which facilities to audit is based on information collected through self-assessments, specific reports made to EthicsLine and other reporting channels, along with risk factors such as activity, location and reputation. New suppliers receive priority attention — as well as those with the largest commercial relationships.

Tier one suppliers are required to monitor their suppliers, with respect to corporate responsibility. Tier one suppliers are also required to provide a list of their suppliers on request. Tier two suppliers are not included in the regular audit schedule, although the company may take part in joint audits with its tier one suppliers in response to specific reports of issues at their suppliers.

Following a supplier audit, the company provides feedback to suppliers and work with them to correct the issues identified. A follow-up audit, conducted by a third party or by its own supply chain team, may be used to verify that suppliers have made the necessary improvements.

The company has established four levels of severity for issues identified through EICC monitoring:

- **Priority Red:** Severe issues that require immediate escalation to our senior management, including child labor, forced labor, slavery, debt labor, illegal dumping of hazardous materials, use of minerals associated with conflict and serious sanitary, health and safety conditions.
- **Priority One:** Legal compliance issues or other issues that represent significant risk.
- **Priority Two:** Non-compliance with contractual terms, our expectations or other applicable codes or standards.
- **Priority Three:** Opportunities for improvement.

In serious cases, suppliers will be placed on "new business hold" — meaning no new business will be placed until the issue is resolved. If a supplier refuses or is unable to cooperate, the relationship is terminated as a last resort. Priority Red requires immediate containment actions to prevent the issue from worsening and to mitigate the negative impact. Corrective action is required at all levels, except Priority Three. Suppliers are asked to provide a date for completion and the company works with them until all issues are resolved. Deadlines are set on a case-by-case basis.

By 2014, the company had completed reviews of 226 suppliers amounting to 66 percent of total spend. Of these, 137 were manufacturing suppliers (59 percent of spend) and 89 were field service contractors (7 percent of spend).

Conclusion

Following the major reorganization of the company, the supply chain and procurement organizations initiated and made great strides in their transformation efforts, particularly in when it comes to managing vendor risk. According to the Senior Manager of Supply Chain Operations Strategy team, however, their journey is not over:

> "We continue to look for ways to both improve the process of managing SCRM, as well as reducing overall risk. A simpler process to track, report and train lends to more time that can be allocated to mitigating risks as opposed to just understanding what they are."