

APICS INSIGHTS AND INNOVATIONS

SUPPLY CHAIN RISK: PROTECT YOUR BUSINESS WITH RISK MANAGEMENT



APICS
SUPPLY CHAIN
COUNCIL

ABOUT THIS REPORT

APICS sought to examine the role that supply chain risk management plays in organizations and how risk management will evolve. The goal overall of the supply chain risk survey was to determine the current real-world practice of supply chain risk at the level of APICS members and customers.

More than 9,000 professionals were invited to participate in the survey, which took place from June through July 2011. The survey results reflect an approximate 6 percent margin of error at a 95 percent confidence level.

The survey results reveal that risk management is still at an early stage of maturity and that there are gaps at the organizational-management level and the supply chain and operations management level. As supply chains become more complex, and as risk occurrence becomes potentially more costly, the importance of risk management increases.

This report is developed by the APICS Supply Chain Council (SCC). Its research reports are based on practitioner surveys that explore trending topics in supply chain and operations management. They include survey results, analysis, tips and best practices to keep you and your organization informed of insights and innovations in supply chain and operations management.



SUPPLY CHAIN RISK

TABLE OF CONTENTS

Executive Summary	5	Perspectives from APICS Magazine	
APICS Research	45	From Standstill to Still in Business	22
		<i>How to keep your warehouse moving during a disaster</i>	
		By Christopher M. Wright	
		Continuity planning solutions can help you manage warehousing and distribution risk	
		System Failure!	29
		<i>A survivor's guide</i>	
		By Shankar Suryanarayanan	
		Streamline contingency planning for your computer systems to avoid serious repercussions.	
		See, Understand, Act	36
		<i>The logistics of successful disaster planning</i>	
		The APICS interview with General Russel L. Honoré	
		Build a defense against disasters with actionable logistics strategies	
		Your Enchanted Supply Chain	42
		<i>The importance of an emergency strategy you can believe in</i>	
		By Philip E. Quigley, CFPIM, PMP	
		Build a strategy based on careful preparation, risk analysis and contingency planning in case of both natural and man-made disasters	

SUPPLY CHAIN RISK: PROTECT YOUR BUSINESS WITH RISK MANAGEMENT

Risk:

The *APICS Dictionary*, 14th Edition, defines supply chain risk as “Decisions and activities that have outcomes that could negatively affect information or goods within a supply chain.”

EXECUTIVE SUMMARY

Combine random disasters and the economic challenges related to the cyclical nature of business—rising and falling demand, market uncertainty and varying levels of trust among supply chain partners—and anyone doing the math can see that business faces constant supply chain risk.

APICS invited 9,000 members and customers to participate in a survey to examine the role that supply chain risk management plays at an organization, encompassing both practical supply chain risk strategy and increasing risk management maturity. The survey evaluated the current state of supply chain risk management at organizations, and assessed how risk management will evolve.

The survey results reveal that risk management is still at an early stage of maturity and that there are gaps at the organizational-management level and the supply chain and operations management level. As supply chains become more complex, and as risk occurrence becomes potentially more costly, the importance of risk management increases.

Several trends emerged as survey responses were analyzed:

- Respondents have concerns about relationships with suppliers and customers. In contrast, distribution and warehousing showed the least risk. The areas of logistics, production and customers had more neutral assessment.
- Organizations reported the phenomenon that supply chain risk practice fades once perception of a risk disappears.
- Respondents reported they mostly knew their supply chains from end to end, including the flow of material into and out of facilities from each node in the chain.
- Many respondents indicated that they could map the physical flow of materials from suppliers, including the location of supplier production facilities, freight facilities and transportation methods used by each supplier.
- Most organizations assign responsibility for supply chain risk to supply chain and materials management departments, and buying and sourcing professionals. Somewhat less common are master planning, distribution and senior management.

Breaking the reactive cycle

Risk management strives to address risk proactively, in advance of problems and also in optimizing organization and supply chain response after a risk occurs. Without risk management, risk awareness and response tend to follow an ineffective reactive cycle:



Many risks appear to follow a lifecycle. Yesterday's simple concerns become today's risks. Today's known risks become tomorrow's lessons learned. This lifecycle reflects the process of human discovery, prediction and management of risk applied to the supply chain.

In contrast, a risk management manager or actor works steadily, proactively and wisely to position the organization and its supply chain against risk, both for tactical and strategic benefit.

The scope of supply chain risk management is extensive and spans all areas of the supply chain. At the tactical level, risk management is the continual activity of detection, measurement and evaluation of potential supply chain disruption caused by all varieties of supply chain risk, emanating both from within or outside the supply chain. Supply chain risk management seeks to manage, control, reduce or eliminate real or potential risk exposure to supply chain performance. Risk is the actual or potentially negative impact on supply chain performance. Effective risk management decreases cost by reducing the probability and impact of supply chain disruption and reduced performance.

Risk management alignment

Effective supply chain risk solutions depend on compatibility with an organization's business strategy and mission statement, product families, markets and supply chain partners. For example, supply chain operations must align with the overall strategy of the organization, or else the supply chain generates risk for the entire organization. For a producer of low-margin commodities with stable, predictable demand, a long, slow and inexpensive supply chain may reduce risk when compared to a short, fast and expensive supply chain. The opposite would be true of an innovative electronics manufacturer serving a boom-and-bust market or customer. Lowering risk in one area of the supply chain may simply shift risk to another area. Due to these complexities, there is no one-size-fits-all approach to supply chain risk management.

Risk management covers the perspectives of both known and unknown risk. Examples of known supply chain risks include process breakdowns, supplier failure, poor material and component quality, and inadequate logistics and distribution capability. Other examples include excessive demand instability, criminal action and natural disasters. While known risks are too numerous to list, known risks are identifiable in advance of their occurrence and generally can be prevented with risk mitigation efforts.

Root causes

To eliminate a risk, a supply chain risk manager must discover the cause of that risk. With a known cause, developing a long-term, effective solution becomes possible. However, finding the cause of risk usually is a difficult task. High complexity, missing information and lack of communication are challenges. One strategy is to develop a history and future projection of the risk. Consider the following questions:

- When did the problem first appear?
- How and why was it noticed?
- Why did it not appear earlier?

To project the risk into the future, ask more questions:

- What enables this risk to persist?
- What dependencies (systems, processes, resources) does the risk have to maintain itself?

With a framework of past and future analysis of the risk in place, a common discovery is that today's risks develop from yesterday's solutions. Solving today's risks might need to wait for tomorrow's solutions. A cycle of solution-risk-solution may emerge. The way past solutions develop into new risk may reveal clues to root causes and blind spots.

For example, consider the problem of legacy mainframe computer systems. In the 1960s and 1970s, such systems were the solution to a tremendous number of operational and information flow problems. But such legacy mainframes gradually increased risks in later years. Aging hardware and programs could not flexibly handle rising data volumes or allow integration with newer systems or dates beyond the year 1999.

Replacement systems gradually eliminated the problem but introduced new risks along the way. The solution-risk-solution cycle of legacy mainframe computers may seem obvious today, but it was not clear for many years. Often, gradual problems or soft risk lack visibility and priority in organizational management.

In the mainframe situation, the supply chain manager must consider and address inattentive management as a cause of supply chain risk. Often, the same management culture may exist, and the supply chain manager must work to dismantle it.

Addressing unknown risk

Supply chain risk management must also address unknown risks. Good practice and preparation is key to improved responsiveness to what is unknown. Unknown risk may be framed or classified in two ways:

- Supply chain assets may face loss due to the unknown risk
- If loss occurs, the level of damage mitigation and post-risk response that is required also serves as a classification

For example, suppose an unknown sinkhole, impossible to detect in advance, were about to open up beneath the floor of a production facility. The sinkhole remains an unknown risk until it occurs. However, an organization that possesses risk management strategies that address (1) loss of use of the production facility, and (2) rapid replacement of production capability, could apply those plans to the sinkhole risk once it appears.

Preparing for and addressing unknown risks can partially occur by identifying soft risks, which are those risks that are difficult to clearly detect and measure, but which may increase the odds of negative impact or loss. Note: See the “Practice scenarios” section for more information about soft risk.

Using the sinkhole example, (1) a soft risk might be the cutback of physical facility inspections due to budget cuts, and (2) the expectation of sinkhole-related loss based on the history or statistical study of the types of building losses experienced in the area of the production facility. Post-risk mitigation efforts of all kinds generally improve when the supply chain has a track record of ongoing, effective levels of proactive and reactive risk management practice.

New aspects of supply chain risk management

Historically, costs devoted to supply chain risk reduction rarely exceed the cost of expected losses in the supply chain. There seemed to be little strategic added value for additional spending. However, this perspective is changing. Risk management increasingly is recognized as creating a strategic competitive advantage. It promotes an agile supply chain that:

- Outperforms competitors impacted by the same shared risks, thus boosting market share when a sudden common risk occurs
- Supports optimal supply chain design by reducing uncertainty and strengthening relationships and trust to reduce risk
- Continually detects, optimizes and reduces risk exposure and cost when compared to competing supply chains

Supply chain risk management develops the concept of co-destiny. The APICS Dictionary, 14th Edition, defines co-destiny as “The evolution of a supply chain from intraorganizational management to interorganizational management.” With regard to co-destiny, supply chain risk management pursues both prevention of risk and loss mitigation of post risk events. The entire supply chain benefits from risk discovery and reduction at every point.

The supply chain manager that considers risk must serve as the awareness champion of soft risk and gradual problems. To act as champion means to know risk cause and history, the threat over time, and the ideal way of addressing risks with minimal outlay bound by organization budget and strategy. Risk reduction frequently comes at the expense of resources and flexibility.

A supply chain risk manager must be able to demonstrate why reducing risk is worth the lost opportunity cost of resources or reduced flexibility, and how the risk mitigation tactic promotes organizational and supply chain strategy. To accomplish this, the supply chain risk manager must have an excellent understanding of organization and supply chain strategy and how risk reduction serves strategic needs. Note: See the *APICS Supply Chain Strategy Folio: Make the Most of Supply Chain Strategy* for additional strategy information.

Current practice and maturity levels

Supply chain risk management is not as advanced as other operations management disciplines. Standard forms of reporting, vocabulary, mapping and conceptualizing supply chain risk are not complete or have not yet been universally adopted. Even with easily measurable risk data, supply chain complexity makes it a challenge to gather a complete, intricate view of a supply chain's total risk profile. Of course, not all supply chain risks are easily measurable.

Risk management may involve non-intuitive processes or analysis across many stakeholders. Nonetheless, the level of risk management's visibility and integration in an organization is a sign of its maturity level. Integrating supply chain risk management with business continuity, security or planning departments may assist its integration, especially in an industry such as finance.

Most organizations find themselves somewhere in the middle of the following continuum:

- There is no supply chain risk management in place.
- Formal or informal risk management happens when a clear threat appears, but efforts fade as the hazard disappears.
- A formal position or positions address supply chain risk, but efforts are mainly tactical and focus on specific areas of the supply chain, not the entire supply chain. Visibility is not optimal across the organization or the supply chain. Supply chain risk management is not widely regarded as a strategic competitive advantage.
- There is a formal cross-departmental team or group to address supply chain risk across the entire supply chain. The team or group successfully maintains visibility and awareness with the rest of the organization and supply chain. Supply chain risk management is generally acknowledged as a strategic competitive advantage.

Getting started: Supply chain risk tools of the trade

Often, despite development of risk management plans and lists of risks and threats, supply chain operation remains unaffected. When a risk finally occurs, the typical stakeholder or manager response is, “How did this happen? Why weren’t we prepared?” These questions and similar cries for risk information should be answered well in advance.

The first step is building up risk awareness. Effective risk management develops risk awareness across elements of the organization—from senior management to department heads and middle managers.

Begin by creating a senior-management sponsored cross-functional, supply chain risk team that develops and reports across the organization. Reports should include a complete perspective of the organization’s business, supply chain dependencies and operations. The group’s purpose is to build an effective supply chain risk portfolio that includes:

- Supply chain risk profiles
- Practice scenarios
- Risk checklists
- Supply chain risk software and tools
- Emergency and crisis management plans
- Risk management tactics and strategies

Supply chain risk profiles

With an experienced and representative stakeholder group, a list of known supply chain risks can be compiled. Then, a risk profile catalog should be built, which is done by continuing the consensus approach. First, give each risk an initial priority pass, classifying each as important or not important and urgent or not urgent.

Important and urgent are different concepts. Plenty of urgent tasks demand immediate attention but are not important (for example, scratching an itchy mosquito bite). In risk management, urgent but unimportant tasks are usually distractions or interruptions, such as an email insisting on an immediate response to a minor issue. Likewise, important tasks may not be urgent. Completing a report on inventory loss may be important but have a due date of 10 months into the future. Prioritizing current and future risk management efforts requires attention to both important and urgent measurements.

Important and urgent tasks have a high priority. At this point, human nature tends to assign urgent but not important risks as moment-to-moment priorities, while ignoring important but not urgent risks. A risk management process helps overcome human nature and ensures important but not urgent risks receive a fair share of attention before they become important and urgent.

First, create a risk management list. Prioritize your list, and drop all risks identified as not important and not urgent. Then, classify each risk according to probability and consequence:



Then, add a time period and data to each risk.

Select risks that exist in a defined period of time (such as month, quarter or year), identify their owners, and include value-add estimates.

Quantifying risk profiles

A risk profile can be quantified by assigning individual posts such as (1) for low, (2) for medium and (3) for high, to both the probability of occurrence and the consequence of risk occurrence. Multiplying probability and consequence points results in total severity point value. This helps prioritize risk management efforts.

This table is an example of a current quarter supply chain risk profile for a fictional company.

Risk name	Owner	Probability points	Consequence points	Total severity points
IT system fails	IT	Low: 1	High: 3	(1x3)=3
Key supplier strike	Buyers	Medium: 2	High: 3	(2x3)=6
Hail damage	Facilities	Low: 1	Low: 1	(1x1)=1
Obsolete inventory	Production	High: 3	High: 3	(3x3)=9
Unrealistic key customer demands	Sales	Low: 1	Medium: 2	(1x2)=2

It is simple to refine the risk profile to consider expected loss in currency, units of production or customer satisfaction. The team may choose to replace the simple high or low probability of occurrence options with actual percentage probabilities calculated from other sources—such as a 65 percent chance of occurrence rather than high or low.

Risk profile tables create historic, quantifiable data to chart and evaluate for repeating visits or risks correlated with seasons, suppliers, customers or other elements of the supply chain. Overall risk trends or a combined risk profile for the supply chain becomes possible with a variety of risk profile tables. Participants must ensure the risk profile process occurs frequently enough to track high probability and high consequence risks to prevent surprise among stakeholders and to provide timely mitigation opportunity among owners and stakeholders, who should be actively participating in the development. Consensus is key. Remember: A lack of involvement usually means no commitment to reduce or mitigate risk.

Practice scenarios

Practice scenarios are akin to fire drills. They simulate a risk occurrence and measure the performance of all participants. Their purpose is engagement, education and the discovery of lurking risks. Practice scenarios are particularly useful for risks that reveal themselves only in practice, but otherwise remain hard to spot. For example, when a hard risk manifests itself and causes harm or damage, there will be high demand for information, speed, communication, alternative analysis, damage assessment and mitigation, investigation and reporting. How do the stakeholders respond to this out-of-the-ordinary situation? Practice scenarios probe for weakness and help reveal less-than-optimal responses.

Practice scenarios are also effective on soft risks. Soft risks are those risks that are difficult to measure or perceive. Weak leadership on the part of senior managers is a typical example of a soft risk. While this type of soft risk is hard to identify, conducting practice scenarios results in the appearance of indicators such as confusion or lack of decision-making authority.

Practice scenarios show when a risk brings about harm or damage and likely will trigger additional risks, causing a ripple effect of increasing risk exposure. Rapid and coordinated damage control helps minimize this problem. Damage control should also be a function of practice drills and scenarios. What works and what fails becomes clear, as do differences between an optimal response and a less-than-optimal response.

Risk reduction checklists

Prepared in advance, risk reduction checklists ensure that an optimal sequence of tasks and stakeholders prevent risk and catalog risk prevention steps. Supply chain professionals should establish checklists for routine operations, such as evaluating performance and maintaining relationships:

- A record of a completed checklist on file can make a significant difference when investigating the causes of damage from an unknown or unexpected risk.
- Completed checklists help ensure soft risk mitigation and risk management culture remain ongoing priorities of an organization.
- Checklists ensure objective measurement of situations that may suffer from incomplete, faulty or subjective perceptions.

Consider developing objective, standards-based checklists for high-stakes or important supply chain tasks such as selecting and adding new suppliers. Checklists help make risks visible to everyone. When checklists are developed and shared with other parties in advance, clear expectations frequently replace misunderstanding.

Supply chain risk software and accreditation

Some organizations map their supply chains using flow-charting software. A variety of supply-chain flowchart templates help capture simple supply chain risk relationships. Currently, research and development is underway for tools that mine available transaction information, tracking supply chain components, near real time performance and materials flow. Still, relatively few organizations enjoy this capability because it requires extensive custom information systems development.

Government- and industry-sponsored supply chain risk standards and certifications programs create public-private models of supply chain risk framework and practice. These usually involve customs, law enforcement, border security or similar national officials. Tested or accredited supply chain participants typically agree to maintain program standards and pass information on the movement of goods before they leave or enter a region. These programs enable authorities and stakeholders across the globe to cooperate and carry out better risk analysis. For example, before or after goods arrive in the customs territory, general and specific risks are managed thanks to early availability of risk-related information.

The following are examples of these types of programs:

- **United States:** Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep) and Customs-Trade Partnership Against Terrorism (C-TPAT) www.fema.gov/privatesector/preparedness
- **European Union:** Authorized Economic Operator (AEO) certification for supply chain security and EC Regulation 648/2005 ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/aeo/index_en.htm
- **Industry:** Transported Asset Protection Association (TAPA) and TSR-2008 accreditation www.tapaonline.org/
- **Industry:** International Organization for Standardization (ISO), ISO 31000–Risk Management www.iso.org/iso/iso_catalogue/management_and_leadership_standards/risk_management.htm

According to the *APICS Operations Management Body of Knowledge (OMBOK) Framework*, risk management covers supply chain risks that can be categorized across two dimensions:

- **Coordination risks:** Risks associated with the day-to-day management of the supply chain, which are normally addressed using principles such as safety stock, safety lead time and overtime
- **Disruption risks:** Risks caused by natural or man-made disasters such as earthquakes, hurricanes and terrorism.

Supply chain risk management is evolving

Increasingly, there are formal roles devoted to risk management, or it becomes a formal responsibility of existing supply chains, materials and operational management roles. This trend stems from the rising visibility of supply chain risk. The natural disasters the globe has seen over the last several years, as well as increasing information technology capabilities, have demonstrated to business management the rewards that are available through the practice of risk management.

Particularly in challenging economic times, risk management can help an organization endure and even benefit from risk, at the expense of its competitors that are not so well versed in risk management. Consider the industry and media attention given to risk management after the major natural disasters of the last five to 10 years, from Hurricane Katrina to the earthquake and tsunami in Japan. Visibility of risk management tends to rise and fall with reported disasters. However, formal ongoing roles and responsibilities help counter the cyclical rising and falling attention given to risk management as risks occur.

Why is supply chain risk management Important?

- **Risk management stimulates many supply best practices.** For example, risk management is a key stakeholder in eliminating waste. The use of resources or assets creates inherent risk. Use or deployment of wasteful resources creates unnecessary additional risk to the organization, as well as to the supply chain. Risk to even a wasteful resource or asset may potentially compound losses in other assets should risk occur.
- **Risk management generally improves supply chain partner relationships** as joint risk sharing and risk information improve, and through increasing trust as risk management practice demonstrates commitment and capability the supply chain can count on.
- **It provides visibility of supply chain-wide risk**, ascertaining the reality of constant risk exposure not only within the network of a single organization's facilities, but across a broader domain of geographies and capabilities.
- **The reality of soft risk—risk that is difficult to measure—and its unintended consequences in business management.** There is a need for constant awareness and vigilance toward decisions, processes, practices and goals that may unintentionally increase or decrease in the supply chain.
- **Every business faces the balance point of risk and reward.** Over the course of history earning a greater reward generally requires enduring a greater risk. Risk management ensures that risk exposure is optimally minimized while the organization seeks its greatest reward from its people, assets, capabilities and resources.

Gain competitive advantage through risk management

Improved risk management enables an organization to take market share from competitors when a common risk strikes, and leads to improvements in discovering, preventing and addressing smaller risks, which may cost effort, expense or time. These benefits increase when practiced across a supply chain. A supply chain practicing risk management is faster to spot risk, faster to respond to it and faster to claim advantages from these capabilities. Competitor supply chains and organizations may not have as well developed risk management practices. This becomes a key strategic competitive advantage even for commodity product producers.

Supply chain risk management maturity highlights

Risk management practices and perspectives	Organizations practicing risk management less than two years	Organizations practicing risk management for more than 10 years
Does your organization have a formal supply chain risk management job role or position?	Yes: 3%	Yes: 30%
Does your organization simulate or role-play supply chain risk scenarios?	Yes: 18%	Yes: 40%
Which risk is most likely to affect your supply chain?	Lack of supply chain information sharing	Natural disaster disruption
Do you have a crisis mitigation plan in place right now?	Yes: 33%	Yes: 70%
What reports, measurements or metrics do you use to evaluate supply chain risk?	Information flow: 20% Inventory levels: 42%	Information flow: 60% Inventory levels: 85%
Have you personally experienced a major supply chain risk situation?	Yes: 32%	Yes: 48%
Are you always aware of supply chain risk?	Yes: 7%	Yes: 39%

Survey participants were asked the following question: “If your employer assigned you to serve in a supply chain risk role, what challenges do you foresee?” More than 60 percent of all respondents indicated lack of resources, useful tools, data or platforms to capture, analyze and integrate supply chain risk into the existing supply chain management processes.

Further, concern about soft risk—risk that is not easy to measure—was apparent. Between 25 percent and 50 percent of respondents indicated the following areas of concern:

- Growing uncertainty because of changing laws, regulations or liabilities.
- Slow supply chain performance compared to competitors.
- Focus on efficiency at the expense of risk responsiveness.

These results suggest operations management professionals are in a unique situation to influence the level of risk management maturity in their organizations. Their direct access to supply chain information and function combined with responsibility for risk management, position them to serve as formal or informal risk management practitioners.



Adams St

S. Riverside Dr

STOP

PERSPECTIVES FROM APICS MAGAZINE

APICS magazine is an award-winning publication featuring innovative ideas and real-world strategies for inventory, materials, production and supply chain management; planning and scheduling; purchasing; logistics; warehousing; transportation and logistics; and more. Visit apics.org/magazine to view current and archived issues and to learn more about the magazine.



FROM STANDSTILL TO STILL IN BUSINESS

How to keep your warehouse moving
during a disaster.

By Christopher M. Wright



Imagine being woken up by a 6 a.m. phone call informing you that the oil depot next to your business has just exploded and your only warehouse is engulfed in flames. Oh, and the sole copy of your disaster recovery plan is inside. Oops.

There is no shortage of natural and man-made disasters that can and do befall distribution centers everywhere. Earthquakes, hurricanes, tornadoes, chemical spills and flu pandemics all can put a warehouse out of commission.

Fire is the number one loss Richard Luongo sees from warehouse claimants, usually from smoking or hot work such as welding. Luongo is vice president and executive technical specialist at the Chubb Group of Insurance Companies. “Because there’s so much combustible material stored in a finite area, usually to a very significant height, it tends to cause a very great fire,” he explains. Damage from natural disasters is another common loss scenario.

Insurance may compensate for some losses, but it cannot by itself restore your business to normal with the same customer base or market share after an event. That takes planning. “You can beat the odds; but why would you take that gamble?” asks Edward Brown III, president and chief executive officer of KETCHConsulting. Brown served as vice president of the APICS Pittsburgh chapter in the 1970s and has been a continuity professional since the late 1980s.

There are examples of companies that survive a disaster just fine without spending time or money on planning. Still, it’s best to be prepared, Luongo says. “If you have a well-authored plan that people have tested and practiced, you’re going to fare better than people who don’t.” For instance, Chubb had policyholders at the World Trade Center who were able to access their plans and successfully restore their businesses after September 11, 2001.

Basic considerations

Have routine inspections to remove cardboard boxes, oily bags and trash. Check sprinkler systems, fire doors and fire extinguishers frequently. Harden the target by upgrading the roof to withstand more wind and snow, providing hurricane shutters for windows or using floodgates or sandbags in a flood plain, for example. Mitigate losses by posting a security guard after an event to prevent overnight looting. Carry property, casualty and business interruption insurance—but plan for delays in settlement and less-than-full reimbursement.

Formal continuity planning has been around for some decades, and the keys to fast recovery have become apparent over time. When asked what makes the biggest difference in how fast a business recovers lost operations, Brian Turley, senior vice president and general manager of software at SunGard Availability Services, answers, “Three things— number one: having documented and tested recovery plans in place that are up to date; number two: having designated core business continuity team members in place who understand their roles and responsibilities; and number three: having good internal communications.”

Following are more specific details on continuity planning musts:

Emergency notification software, temporary teleconferencing capabilities, and an 800 number to update employees are essential. A Web site to keep customers informed and cell phones with area codes outside the city also might be considered.

Team members should be responsible for assigned tasks, such as notifying fire and police, shutting off flammable gases and liquids, controlling ventilation ducts that can serve as pathways for fire, and cleaning up and removing debris. Teams for each shift and backups for each team member are advised.

Because many team members will be operational employees, it only makes sense to include these hands-on planners when planning starts. They understand aspects of the business that front-office people don’t and often will have the best ideas. It almost goes without saying that you need to get commitment from decision makers at the top of the organization. “If you don’t have support, you’re just going to be like a little hamster in a wheel going around in circles,” Luongo says.

Some businesspeople have a disaster recovery plan for their information systems and think that’s the end of the matter. A continuity plan should cover people and processes, as well.

It’s critically important to keep refining your plan and drilling the emergency procedures on a scheduled basis. For example, the National Finance Center in New Orleans continued to produce government payroll checks without missing a beat throughout Katrina and its aftermath because employees had been practicing its plan for 20 years.

Also critical is business impact analysis (BIA). Originally concerned with the financial effects of business outages, BIA now subsumes such topics as reputational impacts and recovery resource identification. But, for Tom Abruzzo — president of TAMP Systems, a continuity software vendor and consultancy in Merrick, New York — the core of BIA remains the amount of time allotted for restoration of business processes following a disaster. The amount selected will, in part, depend on the nature of the business: Are you shipping perishable life-saving drugs or plastic Christmas trees for next December? You need to perform enough BIA to set restoration of processes adequately. “You have to have a target,” Abruzzo says. “Without a target, you can’t plan.”

The less time allotted for recovery, the more expensive the recovery strategy is likely to be. In any event, disaster planning requires some funding, and professionals should budget for it just like any other project. Whether it’s sending people out to look at alternative warehouse space or contracting for equivalent computing capacity, expect to spend some money developing a plan and assembling resources.

There are organizations that spend millions developing big plans and locking in the backup resources needed to handle a disaster. But planning can be as simple as gathering a few colleagues to discuss what risks can hurt you the most, how likely they are to happen, and how far ahead of the game you can get for a couple thousand dollars.

Many people think their choices are limited, and Brown says that’s wrong. He recently presented 18 recovery strategies to a major national retailer with a wide range of price tags. There are many continuity-planning solutions, and not all of them break the bank. Professionals at small firms should think about what will improve their odds of recovery for a reasonable amount of money.

Resources

Contingency planning for warehouse operations should cover, among other things, technology, alternate workspace and transportation. It’s better to research solutions ahead of time instead of after an event. While holding backup resources usually requires putting up some money, you may find it difficult to locate what you need after a widespread disaster if prior arrangements have not been made.

Specifically, consider the following when researching solutions:

- **Disaster strikes and your computers are ashes.** Now what? While IBM and SunGard are the best known for technology continuity solutions, there are myriad approaches and vendors with respect to data, applications and equipment, Brown says. Each has advantages and disadvantages. With enough money, you can guarantee that your computing won't miss a beat — but that might not be necessary for your business. Recovering in six hours might cost 10 times as much as recovering in 24 or 48, he notes.
- **There is always extra warehouse space somewhere,** even in a robust economy, Brown says. Contact a real estate agent, a third-party logistics provider or a distribution facilities lessor to learn about your options. Other choices include reciprocating with a company across town, erecting temporary structures (of varying degrees of canvas and metal), and even fashioning a temporary warehouse out of truck trailers in a secure parking lot. Your carrier might have warehouse capacity of its own or be able to help you find unused capacity among its other customers.
- **What if your drivers are too sick to come to work or your carrier goes offline?** Any number of solutions for moving inbound or outbound cargo is available: renting trucks, switching carriers or even switching modalities. Ask your current carrier about its preparedness activities, and, if you're not satisfied, act accordingly.
- **Suppose a big company has another warehouse 500 miles away with functioning data applications, ample carrier capacity and office space where it can run double shifts.** All set, right? Brown says that's not enough. "It's naive to think that people will go where they're told if their families are in danger just because it's their job. You have to recover the whole person, and that includes the spouse, children and even pets."

It's common to forget that the key ingredient is your employees. As Abruzzo says, "Planning for people's personal needs at time of disaster is extremely important. Today, planners must take that into consideration."

Someone should be available to make employees' travel arrangements, watch children or an elderly grandmother, or even feed the fish, if that's what it takes to staff an out-of-town work site. Providing for employee needs also might entail the distribution of donated food and water or bringing a doctor to the work- place to give tetanus shots and write prescriptions. "The telephone number of a local grief counselor... should be in everybody's plan," Abruzzo adds.

Housing for workers is another key issue, as New Orleanians found out after Katrina. Organizations with alternate work sites out of town had to make

arrangements for hotel rooms and, later on, for apartments and shuttle buses. When stays extended beyond the initial planning horizon, schooling for children became an issue. Housing remained a key concern as employees returned to the city, some to find they had lost their house and everything in it.

Disaster recovery software

Large manufacturing and distribution firms can maintain full situational awareness in perhaps dozens of facilities throughout the world from a single emergency operations center, which runs crisis management software continuously. Such software gives the company one central point for monitoring all business interruptions taking place enterprise-wide and for visualizing the resources being deployed to manage them.

One such software package is Incident Manager powered by WebEOC from SunGard Availability Services (acquired from Strohl Systems and developed in conjunction with Esi). Turley tells the story of a SunGard client whose manufacturing and distribution facilities were struck by wildfires in the western United States. The company had to shut down operations temporarily, relocate employees and restart business processes elsewhere. In effect, Incident Manager moved the situation room online, enabling executives and other responders to follow events and make their reports from wherever they had Internet access.

The ability to manage a crisis remotely is important, Turley adds, because emergencies rarely occur during normal business hours. Incident Manager activates continuity plans, notifies designated personnel, displays employee status and alternate sites, and gathers press releases and other public statements the company has made. A customizable top menu offers instant selection of site evacuation status, critical mission fulfillment, media relations, and other categories of information deemed most important. The software filters out minor events at the local level and escalates the more important ones, such as line or facility shutdowns, for high visibility within the organization. "It prevents a lot of noise from making its way to the top," he says.

One feature that has drawn the most comments is MapTac, which customers can use to mark up photos, maps and floor plans on screen. Professionals can visualize the status of evacuation routes, the location of responding units, and the availability of alternative transportation corridors for getting supplies or cargo in and out.

Another feature customers find useful, Turley says, is Simulator. Actual incidents and the actions taken in response can be archived and played back in their entirety for later analysis. Incident Manager also can build scenarios for training exercises.

Any such software should be flexible and customizable so the functionality is tailored to client needs. The ability to integrate with other modules is another key consideration. There is an advantage to purchasing more than one module or an entire suite from a single vendor. Data, such as employee home and out-of-town contact information, only needs to be entered once. The same goes for important employee attributes, such as the ability to perform cardiopulmonary resuscitation, speak Spanish or drive a commercial vehicle.

Abruzzo recalls the case of one client whose warehouse was damaged. Instead of having to hunt for contractors to fix the roof and other structural problems, the information already had been collected in software provided by TAMP Systems, a Certified Business Continuity Vendor. “They were able to make those phone calls within the first hour- or-so, rather than that taking possibly a day or even more to research,” he says. The emergency notification procedures— based on previously collected cell phone and after-hours numbers for critical decision makers—also saved time.

Although planning software will send initial and updated plans to personal digital assistants automatically, paper copies of the plan should be readily available. “We strongly encourage our customers to have hard copies of all their plans and keep them up-to-date,” Turley says.

Note also that important tasks may fall to a person who has no experience with the software. Turley is on SunGard’s continuity team and keeps a current paper copy of the plan in his briefcase at all times, even when he’s traveling.

Always the unknowns

The ability to respond to emergencies can be a competitive differentiator. Who would you rather do business with—an outfit that never heard of continuity planning or one that has a high degree of sophistication around its planning processes and rehearsal? The question answers itself.

You can’t plan for every eventuality, and things never go according to plan. But, if you plan and drill on a continual basis in a way that is fully integrated with your business, you will have 80 percent of the picture right. As Abruzzo put it, “The only thing more difficult than planning will be explaining why you didn’t.”

Christopher M. Wright is a freelance writer specializing in investment and technology topics for national and international clients. He may be contacted at cwdirect@sinewaveinvestor.com.

SYSTEM FAILURE!

A survivor's guide

By Shankar Suryanarayanan



Most companies have well-documented contingency plans for their computer installations. Elaborate actions, such as hosting by outside experts and intercontinental data backups, are designed to provide protection against fire, earthquakes, hardware crashes, hackers, terrorists and many other real and imagined fears. But, even if none of these possibilities come to life, catastrophe still can strike because of a simple system malfunction—and that is precisely what happened at a consumer goods company for which I worked.

My organization experienced a serious setback when the material requirements planning (MRP) system used for global finished goods inventory started ignoring transit times; specifically, the system made it seem as if a product produced at one location would be available instantaneously at the more than 50 countries around the world in which we conducted business. While this may be every supply chain professional's dream, it definitely was not reality. Our MRP system was saying all was well, even as warehousing professionals were met with widespread stockouts and suppliers reported orders dropping dramatically. What could our team do?

A sinking feeling

While there is a desire to take immediate action in such a situation, it is impossible to launch a war without identifying the enemy. We understood that our supply chain vitals were falling, yet the root cause was unknown. In such times, it is easy to suspect everything—demand spikes, shrinkage, inadequate system performance, poor supplier reliability and much more. However, based on my real-world experience, the following explains exactly where to begin.

1. Make a full disclosure and enlist management support. Be honest about what you are facing, and don't point any fingers. You will be surprised to see how generously people offer their assistance in a crisis situation. In addition, you should:

- Get the executive management team together and detail the symptoms and investigations that are underway
- Make it clear to these leaders that you will do whatever it takes to fix the problem and keep the business running
- Let them know you will ask for additional resources as soon as you know what is required.

Once you eliminate the myriad possibilities and believe that the issue is a system malfunction, you must test rigorously to verify the hunch. When your intuition is proven accurate, you will have to go offline. This is a tough, but necessary, decision and should be made jointly with company executives, users and information technology (IT) team members supporting MRP, as well as anyone else who will be affected by working offline. Keep in mind that the darkest hour is when the decision is made, as it will create considerable apprehension. However, increasing everyone's understanding of the situation, a working manual process, and steady progress every day will lead to significant improvements.

2. Take early action to ensure business continuity. Manual supply chain planning and execution is not a spectator sport. It's necessary to mobilize resources and begin manual processes, involving many different people throughout the organization. Specifically, you should:

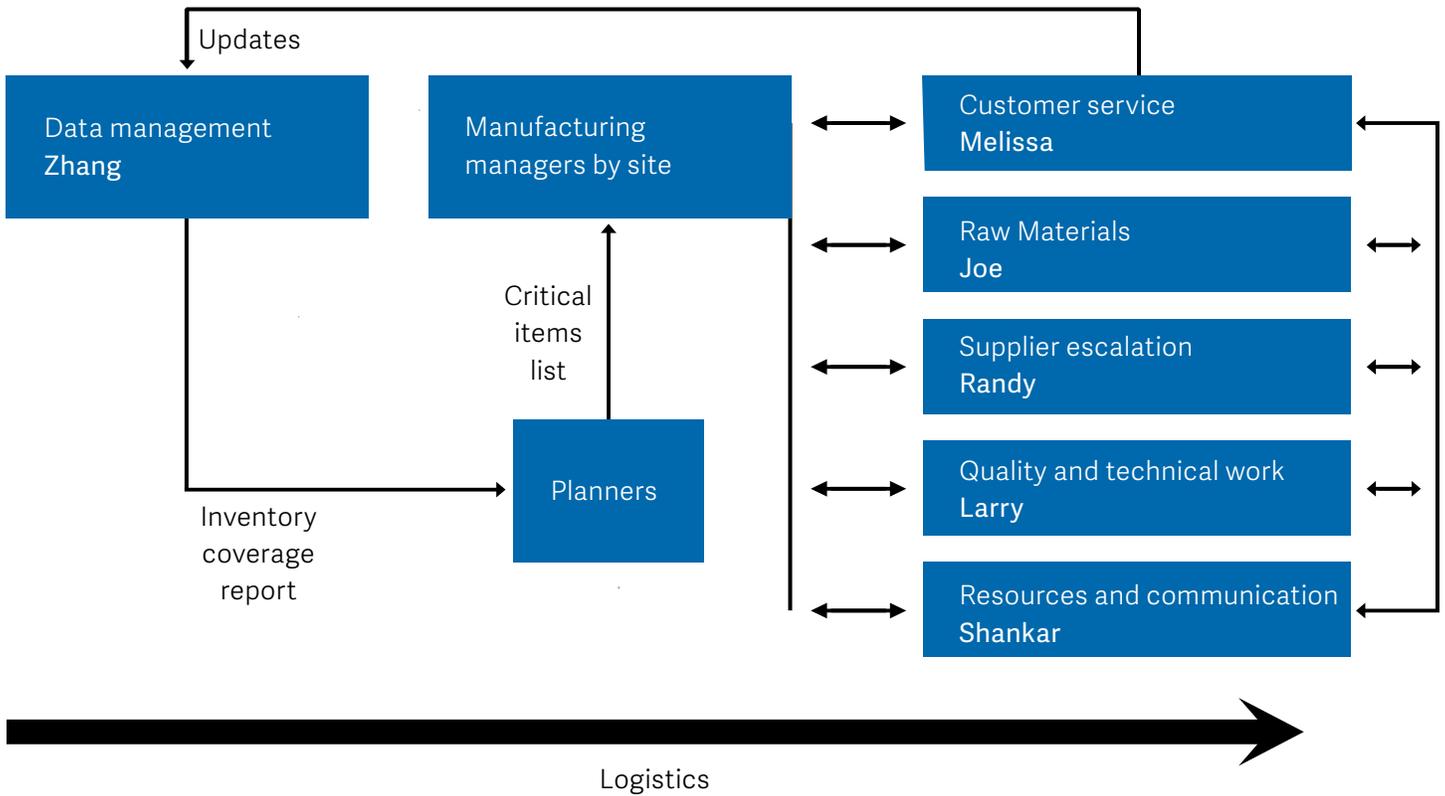
- Quickly put to work consultants and temporary staff
- Immediately get key managers into the "war room"
- Recruit volunteers from other departments for peripheral tasks

At this point, it's time to determine which parts of the system still can be depended on. Next, build an offline tool to help the planners. Perhaps you have old Microsoft Excel or Access software. Now is the time to dust off those tools and find out which colleagues remember "pre-MRP" times.

Throughout the manual process implementation stage, keep in mind the following five guiding principles:

- Manual processes should be built to supplement the capability of key resources, for example, the planners. It's the responsibility of other team members to provide information to the planners in a usable, summarized fashion and then execute the action lists generated by the planners. (See Figure 1.)
- If planners are doing their best, but the manual process proves to be error prone, create tag teams to double-check the work.
- Establish an information repository and daily calendar of meetings and conference calls to keep everyone on the same page. (See Figure 2.)

Figure 1. The manual supply chain planning and execution process



- Identify a point person for each key activity, and publish these contact lists with people’s names, not just their job titles. Impress upon everyone that, regardless of organization hierarchy, people are critically important. All employees must work harder than ever before to make things happen and constantly update the status of their assigned stock keeping units (SKUs), regions and more.
- Anticipate bottlenecks on the path to recovery and get ahead where possible

Figure 2. The manual supply chain planning and execution sample daily calendar

Time	Topics	Participants	Inputs	Actions	Outputs
5:00 a.m.	Data updates	Data managers	Overnight inventory and status updates	Update data and run offline tools	Inventory coverage report by SKU
6:00 a.m.	Planner meeting	Planners and data managers	Inventory coverage report by SKU	Issue purchase order	Critical items list
7:00 a.m.	Update with Europe, Middle East and Africa	Europe, Middle East and Africa and customer service representatives	Critical items for the region	Logistics update, substitutions and expedites	Priorities and to-do lists
7:30 a.m.	Review critical items and create action plan	Planners, customer service representatives, manufacturing managers and logistics professionals	Critical items list	Assign responsibilities	Action item list
11:00 a.m.	Status update by manufacturing site	Manufacturing and materials managers	Critical items list	Review manufacturing and material availability	Additional action items for the day
12:00 p.m.	Update with North America	North America and customer service representatives	Critical items for the region	Logistics update, substitutions and expedites	Priorities and to-do lists
1:00 p.m.	Update with South America	South America and customer service representatives	Critical items for the region	Logistics update, substitutions and expedites	Priorities and to-do lists
3:30 p.m.	Town hall meeting to address issues and prepare for next day	All point people	Feedback on progress and new issues	Review resource allocation	Responsibility assignments
6:00 p.m.	Prepare executive summaries and updates; Update with Asia	Data management; Asia and customer service representatives	Daily activities and results; Critical items for the region	Create communication; Logistics update, substitution and expedites	Priorities and to-do lists
8:00 p.m.	Management update	Vice president of operations	Daily activities and results	Send to leadership team companywide	Key performance indicators, critical items and critical actions

3. Prepare to begin again. Once manual tools and processes are in place, concentrate on reinstating the system. The following actions should be taken:

- Co-locate a team to work on the problem, including users; IT professionals; and consultants from the MRP vendor, who may have overcome similar challenges elsewhere.
- Give a clear mandate to the team and leaders from operations and IT. The team also should have direct access to senior management for regular review of findings and progress.
- Establish a controlled environment for end-to-end testing of multiple business scenarios. The first task is to find out what went wrong, why and since when.
- Review the history of upgrades, patches and parameter changes.
- Once the problems and root cause are identified, outline the solutions. This enables the team to guard against “quick-fix” solutions.
- A plan and timetable should be developed to repair critical problems before the system can start running again. Identify solutions for future issues—these often are complex and require a combination of retraining, reconfiguration and data cleanup.

It is very important to remember that some of the same people will be required to run the manual processes and support system test and recovery. To avoid bottlenecks, use outside resources where possible.

4. Implement preventive measures. Once the crisis is over, begin establishing a program that will help prevent similar problems in the future. Create change-control procedures to ensure cross-functional cooperation during events that could affect system performance. Assign responsibility for periodic system tests—these should be performed under the assumption that nothing works.

It’s also advisable to create joint accountability between users and IT professionals for increased system uptime and accuracy. Review MRP parameters regularly, keeping in mind that actual performance over time may warrant changing system inputs. Plan to create a training calendar, assess skill levels, and designate trainers who will go through advanced training. Finally, review and modify key performance indicators to provide advance future warnings.

5. Look to lessons learned to establish long-term solutions. Create contingency plans to deal with different types of IT system malfunctions. This will enable early detection of problems and smooth the recovery process.

Even after product supplies are restored and the system is reinstated, there will be a long list of things to fix. With managers' attention and willingness to invest in this task, create a roadmap that details how to use IT for maximum benefit. Improvements need not be solely system-based. Think of process, organization and communication improvisations that made things work well during the manual procedures. These should be made permanent—particularly because their benefits already have been demonstrated.

In a crisis situation, it is easy to focus on the tasks at hand and overlook what people are undertaking. This is a big mistake. People's anxiety levels likely will be running very high. Changes in roles and responsibility—and the burden of working in a high-visibility, error-prone environment—take their toll. Make sure volunteers and consultants are welcomed to the team and feel appreciated. Help everyone focus on business continuity by clarifying new roles and responsibilities and explicitly stating which projects and tasks can be put on hold.

Take care of hygiene factors. Employees working extra-long, very stressful hours will need plenty of food available and clean, comfortable office environments.

Lastly, be aware of those who performed extraordinarily well during the crisis and demonstrated knowledge and leadership. Remember to nurture those talents and reward the employees with higher levels of responsibility.

Recognizing the priorities. Running a manual process in crisis mode is clearly not a sustainable endeavor. Preventive measures and regular system testing should be very high priorities at every business. However, following the steps and principles outlined in this article enabled my company to maintain business continuity, while successfully repairing our system issues. Implementing and fine-tuning our manual processes was like a several-months-long kaizen event—it unleashed a lot of commitment, energy and creativity. And, in spite of starting with shortages, we finished the quarter with record revenues and profits.

Shankar Suryanarayanan is an operations management executive who has worked for life science, industrial and consumer goods companies in the United States, Europe and Asia. He may be contacted at sshankar@alum.mit.edu.

SEE, UNDERSTAND, ACT

The logistics of successful disaster planning

The APICS interview with General Russel L. Honoré, U.S. Army (Ret.), Senior Scientist, The Gallup Organization; and Preparedness Contributor, CNN



Editor's note: General Honoré is widely hailed as the "Category 5 General" who led Task Force Katrina in the devastating aftermath of Hurricane Katrina, which struck the Gulf Coast in 2005. Since then, he has written a book on methods of preparedness called *Survival: How a culture of preparedness can save you and your family from disasters*. In addition to his current contributions to the Gallup Organization and CNN, Honoré presented at the 2010 APICS International Conference & Expo. APICS magazine associate editor Ingrid Ostby interviews the general on how to succeed in a crisis using logistics, techniques for preparedness and unflagging leadership.

INGRID OSTBY: What is the first course of action taken after a disaster occurs?

GENERAL HONORÉ: I coined a phrase in the army that still stands: "If logistics was easy, it would be called tactics." It is the hardest thing we do, actually. The success is based on how strong the logistics is... then convincing your supply chain to give you what you need. I can just about tell how a disaster like a hurricane is going to end up by taking a look at how much equipment is on the way there. You know after a hurricane, you're going to need food and water. The federal government waits for someone to ask for food and water.

The dynamics of logistics is how you would use the time and space to get to the right place and right time during the disaster. So, pre-positioning for those annual known events that we're going to have in each region and state is very, very important because the main challenge of getting stuff there is that transportation corridors often are disrupted. They're either underwater or congested with evacuees.

See first, understand first and act first—the logistician that can get his product there from either pre-position or a position close enough to the event, is the one that's going to be the hero at the end of the day. That's what it's all about, because disaster response is about five percent search and rescue, but 95 percent logistics. Food, water and medical [supplies] keep people alive. That's not necessarily what gets most of the attention, but [those are] going to be the biggest requirements.

OSTBY: When you were dealing with the Hurricane Katrina aftermath, what was your biggest logistics challenge?

HONORÉ: Food, water and fuel were the biggest challenges because the supply chain had been disrupted, and the ability to get most carriers at the right place at the right time was a challenge. Also, medicine [was a big challenge] because even though 80 percent of the people had evacuated, the 20 percent that didn't evacuate needed medicine really, really bad. So,

we were starting to evacuate them on medical airplanes because they had gotten sick after the storm because they didn't have medication.

OSTBY: What do you recommend for the future, especially to those companies in locations vulnerable to disasters?

HONORÉ: One of the things I spend a lot of time recommending in my book is that all gas stations and all drug stores should be required to have a generator that can run independently for three to five days, because if people can get gas, they'll leave. If they didn't get the message the first time, they'll get it when they're sitting at their house without power.

The other [recommendation] is if people otherwise are healthy [but] require medication, they can go to the nearest drug store that has a generator that can open up after the storm. That is power because then people can shelter at home.

You will see a lot of problems that you saw during the Washington, D.C., ice storm [in early 2010], where ambulances were having to go get [people] because they couldn't get medication. And most of the drugstores in D.C. didn't have generators and were not open. In a lot of your urban areas, a lot of your corner stores are closed [during disasters]. You'll see a lot of poor people and elderly people actually shopping at these very large pharmaceutical stores—CVS, Rite Aid; they do their grocery shopping there because it's the only corner store in the neighborhood. Because of their dominance and their competitive prices, [these chain stores] put a lot of the small stores out of business. So, it is very important that those stores and your corner gas station, where people buy their bread and beer, have generators. That is the number one thing. If I could create a law tomorrow, I'd require all of them to have that because it adds to the resiliency of the community. If you don't have that, you've got to set logistics camps up like they did down in Haiti with medicine in them. When you put medicine in something, you've got to refrigerate it. [There are] logistics challenges that are caused if you have to keep moving. That's a lot of labor.

OSTBY: What businesses do you think have operated well in the face of a crisis?

HONORÉ: I know large companies that operate down here in the South—the big hardware suppliers—they've got trucks, they watched the storm just like the [National Oceanic and Atmospheric Administration] and the Coast Guard did, and they immediately start moving resupply within the specifics of that storm area. Once it passes, all the plywood that's available and tarps and

water: They've moved all that stuff. When you look at ... Walmart, Home Depot and Lowe's, they move stuff before FEMA [the Federal Emergency Management Agency] moves stuff. That's aggressive. That gets the trucks to the right place at the right time.

OSTBY: Beyond what you've already cited, how else should the business community prepare for risk?

HONORÉ: Number one: Get a prenegotiating contract with your local county government. If you don't have that contract before the event, it's going to be very hard to get one afterward because, when that request goes in, FEMA will send that to somebody from another state to fill. FEMA really doesn't maintain a lot of stock other than a few days' supply of water for a few thousand people. Everything else is ordered after the fact. So, if you're a local supplier or wholesaler ... you have to be preapproved by FEMA and you have to go to their class and get preapproved. Then you go to your county and say, "We'll have the water for you."

You have to have stocks on hand...it is worth the risk to have stocks on hand. You're going to be the supplier of choice. Whereas, a lot of people, they have computer logistics and they don't keep any stocks on hand. Somebody wants something, they order it, and three to four days later, it'll get there. People with supplies on hand are going to make a lot of money [in the face of disaster.]

Let me give you an example. The cost of a truck moving water from Dallas to Houston costs more for the transportation than it does for the water in the back. If you order 10 truckloads out of Dallas, those trucks are about \$1,500 a day to lease. The water in the back isn't worth that much when you're delivering it as an emergency supply. Now, if you delivered it to an airport or to a corner gas station where they sell water for two dollars a bottle, you're not going to get that kind of price if you're a logistician. If FEMA asks you for a truckload of water, they're going to pay you [a fair amount for] a truckload of water; but if you already have that water pre-positioned someplace, then you are going to make a lot of money because you're not paying all that money to move it from Dallas.

OSTBY: You've said that you believe each one of us should be our own personal responder. Can you explain how this might apply to a business setting?

HONORÉ: You need to be your own personal responder because you want to teach businesses to be resilient. Businesses that have resiliency—in other words, they're not waiting for the government to come take care of them—they're used to their level of preparedness so they can open as soon as the

event is over with. That's resiliency. The way businesses [achieve resiliency] is to have organized evacuation and reopening plans.

The idea is to teach people to be survivors and not practice being victims. Businesses that have continuity plans will have a continuation of operation—they will be open first.

There were chain food stores in New Orleans—Burger King, McDonald's—the month after Katrina that were offering people \$5,000 bonuses to go down [to New Orleans] and cook hamburgers and serve sodas, because they went into the storm with no plan for their people. They could have spent \$1,000 by displacing their people before the storm within a couple hundred miles of New Orleans and said, "Okay, as soon as the storm's over, we're going to come pick you up and bring you back so we can open the store." But, the small operators, they didn't think that way. People were all on their own.

A coffee company in New Orleans was roasting about 40 percent of the coffee we consumed inside the United States. Well, that [business owner] took his people up to Shreveport. The day after the storm passed, he rented trucks, everybody pulled the trailer with him, and he went and occupied the parking lot at the coffee company. He never closed his coffee company. Now, that's business continuity planning. That's the power of being resilient in your business: determining how you want to survive.

OSTBY: How far do you think we've come since Katrina in preparing for these sorts of things?

HONORÉ: A lot of people learned. Each generation goes through that. I think government, in a way, has gotten a little better prepared. And the giant companies like Walmart, Lowe's and Home Depot have whole disaster planning teams now because they know the amount of money they can make if they open that store up. It's the small operators that struggle because they don't have the cash flow to be able to keep a lot of stock on hand. They hire temporary workers, and when the mayor says to evacuate, those employees are gone. You can't open your business back up without them.

OSTBY: You've spoken quite a bit about the role of leadership in preparedness. How does somebody heading up a company or task force use that leadership role to make sure everything and everyone is prepared?

HONORÉ: The role of a leader is to create calm out of chaos. They need to get everybody focused on what the priorities are. You can easily become distracted as a leader in a crisis. You've got to think of what did your boss say

was the most important. I think that's what frustrated a lot of people when they saw the reaction of the BP oil spill, because they don't see the priorities carried out.

OSTBY: What's your take on BP's cleanup? Have you contributed to the efforts?

HONORÉ: I am a consultant with the local state and parish officials [and make] recommendations to them on what they should be doing. My first approach was to go about treating the oil spill as a war and come up with a war plan. One phase of the plan [was] to stop the hole, and that was well articulated by everybody. The rest of that plan is how you go from defending the oil on the shoreline to attacking the oil at sea so it doesn't get to the shoreline.

For a long time, the approach by BP and the Coast Guard was just "focus on the hole." They talked very little about what they were doing to prevent the oil from hitting the shoreline. They [received] mixed messages and have not responded in sufficient capacity to the county and state officials who keep asking for more help on the shoreline. They took the other approach of putting chemicals in the water, which diffused the water. We don't know what the long-term impact of that is.

I see the frustration of people along the gulf. They're still confused on the priority of work and who has the authority to make decisions. Right now, unfortunately, too many decisions go back to BP for approval.

For the longest time, it's been clear to me that you can't help the operation because BP [said], "Okay, we got it." But, what you're telling the company to do is not in their trading space—to become purveyors of paying people for the value of their work that they can't do. There are other people in our government that are better suited to do it than BP. Let them focus on the oil and everything associated with oil.

OSTBY: If you could share a single piece of advice with APICS logistics professionals, what would it be?

HONORÉ: Always try to remember that, regardless of the disaster... this is logistics, and how we handle logistics will make a difference in lives saved and damage to people and property. Logisticians have to be involved early on and be a part of the resiliency plan. It's the logisticians that should be calling the shots.

YOUR ENCHANTED SUPPLY CHAIN

The importance of an emerging strategy you can believe in

By Philip E. Quigley, CFPIM, PMP



As I'm writing this, the news is centered on the earthquake in Japan—the loss of life, the physical damage and the nuclear reactor situation have caught the world's attention. In the business press we are seeing stories of plant shutdowns and suppliers' inability to support businesses.

The situation in Japan is just the latest challenge for our global supply chain. There have been storms, earthquakes and fires in China and Taiwan. Middle East political problems still could influence oil prices. There is worry over the new Egyptian government's ability to keep the Suez Canal running. Finally, there is the work of the Panama government in enlarging the Panama Canal and the effect this will have on global shipping.

All of this brings the following questions to mind: Have you planned for problems in your supply chain? Or have you just wished for the supply chain fairy to wave her magic wand, and all will be well? It's amazing how many articles, speeches and books are out there on supply chain strategy; globalization; and the need for careful preparation, risk analysis and contingency planning in case of both natural and man-made disasters. What is even more amazing is how many companies have no real strategy in place to deal with disasters. It seems business leaders at these organizations are, indeed, counting on that supply chain fairy.

For further insights, consider the "consultant test." If I came to your company today and asked for a walk-through or briefing on your supply chain analysis and plan, what would I learn? Specifically, I would want to know who your critical suppliers are; their performance levels with regards to quality, schedule and price; and your grade of these areas ongoing as of last week. Then, I would ask you to tell me about risks, such as the likelihood of these suppliers getting bought out. I'd want to know about their financial strength and the quality of your relationship with them. I would expect you to know about their locations and the associated risks. Finally, I would ask how often you update your plan—and your answer should be once per quarter or per year.

After reviewing the analysis, I would ask to see the specific action plan you have for each supplier. Do you have:

- A list of companies you could shift work to, if necessary
- Estimates of how long it would take to shift work
- An understanding of how much it would cost you?

Build a strategy based on careful preparation, risk analysis and contingency planning in case of both natural and man-made disasters

My final questions would be:

- Who is in charge of monitoring your suppliers?
- And why is he or she the best person for the job?

Your plans could be multiple-page documents or simple checklists of actions. The level of response depends on your company and what it has the resources to do. The key is that you have a plan that comes from some serious thinking based in reality.

How do you get started? First, identify your major suppliers of unique parts or services. They should represent 10 to 25 percent of your supplier network. Next, perform a thorough analysis of these companies. Start with how well they perform their duties. Measure their performance on a week-to-week basis. Then, ask how much research and development they are doing. Determine how long they are likely to stay in business. Are they in danger of a buyout or merger? Finally, consider your suppliers' locations and the types of disaster issues they may face.

Pose these questions to your suppliers in writing and get written responses in return. Create a process for monitoring these businesses, and make sure all plans are up to date.

Inaction is not caused by belief in fairy tales, but by lack of time, resources and money. Make the effort to determine if your organization can handle a major shutdown. Remember: Your company's livelihood depends on what you do right now.

Philip E. Quigley, CFPIM, PMP, is a senior application portfolio manager for Computer Sciences Corporation. He teaches at Chapman University's Argyros School of Business and Economics and California State University at Fullerton. He may be contacted at pquigley2@csc.com or (310) 616-8095.

APICS SUPPLY CHAIN COUNCIL RESEARCH

For more insider information explore APICS research topics at apics.org/research.

Reports are available on:

- Project management
- Remanufacturing
- Risk management
- Supply chain strategy
- Sustainability
- And other topics

If you have comments or questions, contact askapics@apics.org.



ABOUT APICS SUPPLY CHAIN COUNCIL

APICS SCC is a nonprofit organization that advances supply chains through unbiased research, benchmarking and publications. APICS SCC maintains the Supply Chain Operations Reference (SCOR) model, the supply chain management community's most widely accepted framework for evaluating and comparing supply chain activities and performance. APICS SCC enables corporations, academic institutions and public sector organizations to address the ever-changing challenges of managing a global supply chain to elevate supply chain performance. APICS SCC is part of APICS, the premier professional association for supply chain and operations management.

Visit apicsscc.org to learn more.