

Welcome, Jonathan.

Your membership is current until 10/18/2006. | [View/Edit My Info](#) | [Log Out](#)[APICS Dictionary](#)[APICS Learning Communities](#)[APICS Magazine](#)
[Current Issue](#)  
[Back Issues](#)  
[Advertising](#)  
[Subscription](#)  
[General Information](#)
[Best Practices](#)[Buyers' Guide](#)[Career Center](#)
[Job Seekers](#)  
[Employers](#)  
[Career Development](#)  
[Tools](#)
[Consultants Directory](#)[Downloads](#)[e-NEWS](#)[Industry Links](#)[Industry News](#)[Publications Database](#)
[Resources](#) > [APICS Magazine](#) > [February 2006](#) > **TECHNOLOGY'S TREACHERIES**

## Technology's Treacheries

*Identifying vulnerabilities with supply chain continuity planning*
By **JON BELLMAN**

There is a saying, "the best-laid plans of mice and men often go awry." The best-tested plans, however, are less likely to go awry. Vigorous testing is the hallmark of effective disaster planning. While no plan addresses all contingencies, only during battlefield testing are a plan's weaknesses revealed.

Witness Hurricane Katrina. Hurricane plans were in place, but those plans had an Achilles' heel: technology and communications. Systems failed and people died. For example, no one considered, or no one fully planned for, cell phones and personal digital assistants that couldn't be recharged. Testing identifies single points of failure, and the continuity testing process—with its teamwork and its need for innovative thinking and quick decisions—helps to make an organization ready for an event.

Applying modern tools, such as Wi-Fi, Bluetooth, radio frequency identification, and handhelds, to supply chain management enables progressive organizations to gain and maintain a competitive edge. These same organizations are more vulnerable to event-based technology failure than their less progressive competitors. What happens when inventory information becomes inaccessible? Even a noncatastrophic event may greatly compromise an organization's visibility into its supply chain. Without information about inventory, managers often are as paralyzed as if their actual inventory or production assets were destroyed.

Following is a list of technologies that may fail during an event:

- anything with batteries
- alternating current power
- security systems and access controls
- wired and unwired data and voice pathways
- supplier, customer, and other trading partner systems.

Katrina showed little mercy for its victims, no matter who they were. International shipper UPS was heavily affected by the hurricane and subsequent flooding. According to a UPS spokesman, the company lost power and landline and cellular service. Even before the levee break, 53 UPS facilities lost primary data transmission networks, and 31 of those lost their backups. Valero Energy, the largest oil refinery in North America, lost power, and many of its sites were inaccessible. That can be devastating for a company that boasts a 3.3-million-barrel-a-day refining system and 4,700 retail stores.

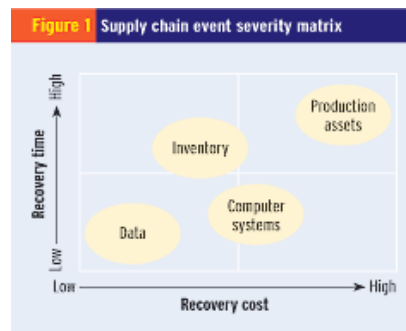
"Forty-three percent of the companies experiencing a disaster never reopen, and an additional 29 percent close within two years," according to the Disaster Recovery Journal. "Seventy-five percent of businesses that lose computer support are no longer able to conduct business functions after only two weeks."

Supply chain organizations rely heavily on their inventory information to help balance international trading relationships and maintain target service levels while minimizing inventory investment. Combining these technologies with enterprise-strength back-office systems creates risk that must be carefully addressed by an organization planning for disaster. Supply chain contingency planners must scrutinize technology and its vulnerabilities.

Thorough planning combined with good testing can go a long way to ensure your inventory data remains available after an event.

### Methods and metrics

The severity and recovery matrix in Figure 1 illustrates the relative recovery costs and time frames for data, computer systems, inventory, and production assets. A minor event may corrupt data and not computer systems or damage inventory but not production assets. A larger event may destroy computer systems, production machinery, buildings, and utility infrastructure. In the hours following a minor event, business data—including purchase orders, production orders, and inventory information—often can be restored from a backup. Backups can be located in an alternate location or in a contracted hot site, which is a backup facility with the information and equipment to allow you to resume operations in a short amount of time. If the computer systems are damaged and restoration capability is not possible, companies may have to bring new computer facilities online.



Event severity and recovery strategies often are described by recovery point objectives (RPOs) and recovery time objectives (RTOs). RPO represents the length of time that a company is willing to lose an asset at normal production or transaction rate. If a company tolerates a prospective loss of two days worth of production or two hours worth of orders from its e-commerce Web site, then its RPOs are two days for product and two hours for data. RTO is the length of time that it takes a company to recover to its normal production or transaction rate. If that same company requires six days to return to normal production and six minutes to bring its Web site into full operational mode, then its RTOs are six days and six minutes, respectively.

RPOs and RTOs are set based on costs, relative risks, and likelihood of gaining or losing market share after an event. Once RPOs and RTOs are specified, companies can provision backup production and computer facilities, purchase business interruption insurance, or increase channel inventory. This is the point when testing is critical. Events are simulated to ensure that planned recovery points and recovery times are achievable.

When measuring a supply chain's event responsiveness, another cliché may come to mind about the weakest link in the chain. Managers should beware that lean-seeking activities designed to reduce inventories and costs may boost scores on traditional metrics, but such actions may increase RPOs or RTOs and lower a company's overall event responsiveness. A healthy respect for variability is critical when considering whether to maintain costs and inventory above the bare minimum to ensure the shelves remain stocked after an event.

Continuity planning must be recognized for what it is intended—to help an organization better manage risk and recover from recoverable events. At some point, organizations find that the cost of insurance exceeds the probability-adjusted impact of the risk. For example, a single-plant company probably couldn't afford a full-capacity, standby production facility 1,000 miles away because the carrying cost of the unused, standby facility would be prohibitive. Intelligent continuity planning is not intended to eliminate exposure, but reduce it when possible.

#### Testing

Rigorous battlefield tests uncover flaws in continuity plans. They enable previously unknown, single points of failure to be identified and addressed. Ernst & Young found that companies with complex supply chains are much more likely to fully test their information technology (IT) continuity plans than their supply chain continuity plans. Ernst & Young also pointed out that ownership for the supply chain plan is often murky and may reside among IT, logistics, and other departments. This makes it difficult to point to an accountable party when planning and testing are inadequate.

The weakest links in the chain rarely are identified during the collaborative and intense discussions that take place during continuity planning. Testing never uncovers all flaws, but the process simulates the real-world stresses through which post-event recovery teams have to work. Leadership, team dynamics, and communications issues can be identified and fixed before an event. Using a "Police Line—Do Not Cross" approach means that you simulate destruction or unavailability of critical business assets and, therefore, don't use them physically or electronically. Monitors evaluate the recovery efforts and stay on the hunt to seek out and eliminate previously unknown single points of failure. This enables critical refinement of the incident response plans before an event, guiding an organization's employees to become more ready in the case of an event.

#### An example

Solovex is a mythical solvents manufacturer located near Charlotte, North Carolina. Last year, Solovex completed a three week continuity planning project with a national consulting firm. The company operates a single plant, employing 600 people. It uses an enterprise resources planning system to manage production and inventory information. It recently replaced its production area personal computers with handhelds.

A hurricane hits and power is gone, so the generators kick in. The cell phone networks become quickly overloaded because both power and telephone poles are down. Power is estimated to be out for 10 days. Solovex keeps enough fuel for the generators on hand, so local power is not a problem. Roads are blocked, and a critical bridge between Solovex and the main road is destroyed (single point of failure). A rain-swollen ceiling collapsed on the main computer room, causing extensive damage. Solovex maintains a contract with a hot site provider that instantly replicates Solovex's data, but the access lines to the hot site run in the same bundle that is attached to the downed telephone poles. Local backups are rotated between the chief information officer's house and

#### Techniques for Addressing Risk

- Eliminate** the risks that are easy to spot and easy to fix.
- Negate** the single points of failure. Create alternatives and backups that can be leveraged after an event.
- Mitigate** unavoidable risks by clarifying post-event roles and responsibilities, both inside your organization and with trading partners.

*For more information on risk, see "Risk Control" (June 2003) or "The Plan Before the Storm" (November/December 2005).*

Solovex's safe, located in the computer room. After the ceiling collapse, the safe is under water.

Creative strategies abound and Solovex's production staff recovers the backup tapes. There is no restore site available, so one will have to be constructed. Version and patch documentation was maintained electronically on a personal computer in the main server room, and no backup was kept. This illustrates a common but fatal flaw that events reveal. While Solovex spent significant money maintaining a hot site, it didn't maintain paper copies of version and patch information.

Three days after the event, inventory data is still unavailable, therefore it is impossible to give customers reliable information. Solovex's plant managers have to interview all of the production workers to reconstruct what was in the company's storage tanks. Certain tanks have capacity gauges that are still functioning, but Solovex's main products are available in different concentrations and blends. The chemists that could manually test the chemicals in the tanks were unable to get into the facility because of the downed bridge. It would take two weeks to get a ferry barge in place and perhaps a week before a helicopter would be available to fly the chemists to the facility.

Solovex executives learned that, as enabling as technology may be before an event, it can be more disabling after an event. Many single points of failure in Solovex's operating model were exposed. Although Solovex had continuity plans in place, decision makers concentrated on protecting the company's most costly assets first, rather than attacking single points of failure. A simple printed document listing patch and version information would have cut three days off the recovery. For a \$500 million manufacturer, three lost days of \$6 million may account for all of the company's net profit in a single year. If Solovex had kept up with an ongoing continuity testing program, it would have been more ready to handle this or any event.

#### **UPS and Valero**

UPS and Valero did their continuity planning homework. They planned and tested their plans. Did their plans cover all contingencies? No, of course they didn't. When Hurricane Katrina hit, both companies supplemented their plans with ingenuity, teamwork, and focused effort.

After the storm, UPS's national system for tracking packages remained operational, and UPS was able to inform its customers about the package status. To restore data in the damaged facilities, UPS's engineers reprogrammed and converted their voice-network routers and switches to accommodate data transfer. These routers and switches were then linked to UPS's still-operational, long-distance carriers after bypassing the nonoperational local phone carriers. In its heavily damaged New Orleans area facilities, UPS employees rekeyed data from paper receipts on to compact disks. UPS employees drove the disks by car, when possible, to locations where the data could be uploaded into UPS's master tracking system.

Valero energy used satellite phones and Internet connections to bring its 14 convenience stores in the Katrina-afflicted area back online quickly to serve customers with food, ice, and fuel. These customers might otherwise have had no access to basic supplies. Valero repurposed an Internet phone switch at its St. Charles oil refinery and converted it for voice use. Valero scrambled IT personnel from nonaffected areas to support the recovery efforts. It took 10 days for landline phone service to be restored to its St. Charles facility, but Valero wasn't waiting by the phone. The company's event-ready organization already was using its workarounds, both planned and newly improvised, to get back online.

UPS and Valero both planned for disaster. Neither company is out of business because of Hurricane Katrina, despite the extreme severity of the event.

When organizations become dependent on technology as a lifeline, that technology often acts as a noose, especially when testing has been inadequate. An organization relying on RFID to manage inventory, for example, must have a plan in place to ensure inventory data is available after an event. The learning that takes place via testing enables an organization to improve both its continuity plans and event responsiveness. Thick binders of dated, untested continuity plans are much less helpful after an event than an event-ready team that has learned to keep extra batteries on hand.

#### **Test Yourself**

Here are five critical, low-cost tests that your organization can run to ensure your supply chain is ready to withstand a damaging event.

- Perform a complete data restoration to your company's recovery servers using your last full system backup, and evaluate whether data is usable and accurate.
- Check batteries and chargers to gauge length of service that will be available after an event.
- Review phone and data contingency plans to ensure that communications will be available after an event.
- Isolate critical staff and ensure that alternate recovery personnel have access to passwords and the required security clearances to restore technology operations.
- Check your insurance coverage and test your carrier's responsiveness while not using your systems electronically or physically.

---

*Jon Bellman founded Reality Check LLC in 1997 and has helped more than 50 companies solve management and technology problems. He is a guest lecturer and speaker at universities and industry conferences. He may be contacted at (212) 580-2315 or [jbelleman@rcheck.com](mailto:jbelleman@rcheck.com).*



[About APICS](#) | [Bookstore](#) | [Certification](#) | [Education](#) | [Membership](#) | [Resources](#) | [Join](#) | [Contact Us](#) | [Site map](#)

[Terms of Use](#) | [APICS' Privacy Policy](#)

All contents © 2006 APICS. All rights reserved.