**Bloomberg Businessweek**

# Technology

http://www.businessweek.com/articles/2012-12-04/the-importance-of-disaster-plans

# The Importance of Disaster Plans

By Verne Kopytoff December 04, 2012

After several close calls with hurricanes, executives at Florida Hospital in Orlando decided to rethink their disaster plans. A direct hit by a storm could, of course, endanger patients. But it could also destroy the technology that the facility depends on for medical records, clinical test results, and accounting. With strict regulations about hospital safety and the critical nature of the facility's services, nothing could be left to chance. The hospital came up with a comprehensive strategy to prepare for future disasters, reengineering how it safeguarded its digital records and reserving backup offices.

"In 2004 we had what we called the hurricane trifecta—Charlie, Francis, and Jeanne," says Robert Goodman, disaster recovery coordinator for Florida Hospital. "The hurricanes got our management's attention."

Disaster planning plays an important role for businesses in ensuring they can still operate after an earthquake, a blackout, or other serious disruption. Failing to prepare can mean millions of dollars in losses and major headaches while trying to recover. As a precaution, many companies draw up what are known as business continuity plans, which provide a road map for responding to a variety of problems. The first step is invariably to identify critical assets such as manufacturing facilities, technology infrastructure, and corporate data. The next step is to figure out how to protect them—or at least minimize downtime—amid bad weather, labor strikes, or cyber-attacks.

Planning should not be limited just to a company's own operations. Key partners and suppliers could also run into trouble. For example, companies are increasingly using software in the cloud—services provided by third parties from remote data centers. What if such a vendor went offline?

Nearly three-quarters of all companies have a business continuity plan, according to a survey of 300 executives conducted last year by *Disaster Recovery Journal*, an industry publication, and consulting firm Forrester Research (FORR). Government regulations all but require such plans in critical industries like health care, energy, and finance.

Technology almost always plays a prominent role. Ensuring that key computer systems operate during and after disasters has evolved into a mini-industry with armies of consultants and vendors. Shoring up technology against disruptions can be costly. Companies will spend an average 7 percent of their IT budgets on business continuity and disaster recovery this year, according to Forrester.

Al Berman, president of DRI International, a nonprofit certification organization for the disaster recovery industry, says that in light of the cost, companies must set priorities. They may be able to live without access to certain software for a few days, for instance, or entire lines of business.

"Some companies say, 'We want to service our five biggest customers—and let the others go,'" Berman says. "Or they want to preserve their highest-margin business and let the other ones go."

Florida Hospital, which has more than 20 facilities across central Florida, has prepared for disaster by backing up its critical records at a data center 1,000 miles away in the Northeast. (The hospital declined to name the location for security reasons.) If its primary data center in Orlando is taken down by a hurricane, employees will still be able to access information via the secondary facility.

SunGard, a company that specializes in disaster recovery services, operates the backup facility. In addition to storing the hospital's data, SunGard technical staff will help get the hospital's records back online if a disaster strikes. The job of restoring the data should take around four to six hours, Florida Hospital's Goodman says. At worst, a few minutes' worth of new data may be lost after the primary servers go down, he explains.

Previously the hospital relied on an unwieldy system in which it saved data to tapes and delivered them by truck to another backup facility in the Northeast. When a hurricane approached, the hospital staff would have to scramble to get 2,000 tapes ready and then wait a couple of days for them to arrive at their destination. By the time the data could be restored, it would be several days old.

"You would run into a situation where you would go look up a lab order and couldn't even see that the patient was ever admitted," Goodman says.

Testing is key to ensuring that data recovery plans work when needed, no matter the kind of business. Florida Hospital conducts two tests annually, during which it simulates a crash at its primary data center in an effort to find bugs. "When we do an exercise, we expect to have problems," Goodman says. "We are trying to learn what we don't know."

In a sign of how it has simplified its procedures, the hospital recently sent only a handful of employees to its backup data center for the exercise, and intends to winnow that number down further in the future. In the past, it would require as many as 20 workers.

"I'd much rather be in Orlando helping my family and the business," Goodman says.

As with most data centers, Florida Hospital's primary facility in Orlando has formidable defenses. Housed in concrete, it's built to withstand winds of up to 145 miles per hour. Electricity from two different substations goes into the building so that if one of the substations goes down, the other can take over. For extra safety the hospital has, as part of its contract with SunGard, arranged for a trailer filled with servers to be delivered to its campus if its data center is damaged. The trailer's equipment would serve as a replacement until the hospital could make repairs.

As another precaution, the hospital has lined up office space through SunGard in a disaster-resistant building near Orlando in case some of its own offices are damaged. The space, called a business recovery center, comes with a secure telecommunications system, backup generators, and hundreds of empty desks.

Warren Zafrin, managing partner for SunGard, says companies can't anticipate everything. Moreover, they continually create new vulnerabilities by adding technology, offices, and by moving into new businesses.

"With Sandy, people are realizing that their plans didn't account for everything or that their business changed dramatically," Zafrin says. "The technology that they use changes. Plans have to keep pace with it, and that's

where a lot of companies fall down."

Kopytoff is a *Bloomberg Businessweek* contributor in San Francisco.

---