MARCH 1, 2006 | CIO MAGAZINE

DISASTER RECOVERY

Captain Contingency

MIT logistics expert Yossi Sheffi talks with CIO about what companies can do to recover quickly from almost any type of disaster.

BY SUSANNAH PATTON

When the South Tower of the World Trade Center collapsed on Deutsche Bank's New York facility, the German banking giant lost its connection to the U.S. markets. Almost immediately, however, backup systems in Ireland kicked in, and Deutsche Bank went on to clear more than $300 billion in transactions that same day.

After the September 11th attacks, and more recently hurricanes Katrina and Rita, companies such as Deutsche Bank have been able to bounce back because they planned for the unthinkable. Yossi Sheffi, director of MIT's Center for Transportation and Logistics, calls these organizations "resilient."

In his recent book, *The Resilient Enterprise*, Sheffi says companies and government agencies need to take a systematic approach to disaster planning. (Read an excerpt from his book.) The list of things that can go wrong is endless, especially in this age of supply chains that stretch around the globe, leaving companies vulnerable to strikes, natural disasters and civil unrest far from home base. Companies need to start cataloging what could go wrong, but they also need to examine their cultures to make sure theirs is resilient. Companies that recover in the face of devastation are those with redundant systems, but they also empower all levels of employees and create a sense of passion for work, Sheffi says. Company cultures that promote resiliency should be equipped to respond to almost any disaster.

Resilience through Redundancy

An excerpt from Yossi Sheffi's recent book, The Resilient Enterprise.

Read More

Building redundant IT systems is most important for technology-intensive industries such as financial services. But even universities and other organizations with less pressing need for immediate backup should evaluate which types of data are most crucial to their daily operations. It's a simple equation, Sheffi says. "It's better to pay something now, than to possibly lose your business in the future," he says. Sheffi recently spoke with *CIO* about what makes companies resilient and how CIOs can build a case for a comprehensive plan to keep IT systems up and running when the unthinkable strikes again.

CIO: Several recent disasters have shown that companies and their IT leaders need to be prepared for the unknown. What have we learned, for instance, from Hurricane Katrina?

Yossi Sheffi: We've learned that the fates of companies and government agencies are sealed before the disaster hits. Organizations that get ready perform well; those that don't prepare don't do well.

Just look at FEMA. They were hiring people with no qualifications, and they had not set up adequate communication systems. This was happening for years. And New Orleans had not responded to warnings three days before the storm hit. On the flip side, we should look at Wal-Mart and Home Depot, which responded quickly. They have both spent years building up their emergency room and communications systems so they can respond to any natural disaster. These companies are able to change course when conditions change abruptly.

What should companies be doing right now to emulate Wal-Mart and Home Depot?

They need to look at company culture. There is something in the DNA of resilient companies that is missing from those that falter and suffer. It goes beyond just redundancy. First of all, communication is key, and I've found that resilient companies communicate obsessively. The U.S. Navy is a good example. On aircraft carriers, there are lots of so-called listening networks that allow lots of people to listen to communication between pilots, the tower and the landing signal officers and others. It may sound like a lot of chatter, but everyone is listening intently so they can react immediately if something goes wrong.

Another factor is empowerment. At Toyota, for example, every worker can pull a cord and stop production if they see a quality problem. If they pull it, the line stops and a team of engineers descend to see what is going wrong instead of just letting the line keep working. This is an effort to prevent the making of bad cars. The same thing happens on a Navy carrier, where every sailor on deck has the right and responsibility to stop flight operations if they see a problem developing. This is amazing because you're talking about what could be a 19-year-old with one year of training having the right to stop a multibillion-dollar ship with 6,000 highly trained sailors on deck. In disasters, it's clear that you have to react immediately, and it's possible that one sailor could see it coming.

The third characteristic of good culture is a passion for work. Navy sailors, for example, don't think about their job as driving big ships, they think of their job as defending freedom.

How has globalization made companies and their IT systems more vulnerable when disaster hits?

Globalization of the supply chain is still marching on because labor costs are so low in places like China. But this trend stretches the supply chain across the globe and makes companies vulnerable. Lead times are longer, and a lot can happen in the meantime. It takes six to eight weeks to go over the ocean and during that time, demand can change. And, more importantly, risks such as theft and counterfeiting rise. Also, many regimes are unstable, and there are unpredictable events such as strikes and terrorism. All of this creates a more brittle supply chain. When something goes down and the transportation link breaks, the product is just not available.

There are ways to protect yourself, however. When it comes to IT, the need for redundancy is obvious. The cost of an information technology outage to a major corporation from floods, terrorism or whatever, is huge. It can put the company out of business. But the cost of backup and redundancy in IT is relatively low, especially when you compare it to having a redundant manufacturing plant.

Is there a difference between redundancy and mere backup?

Redundancy is more than the backup of data. Redundancy may require, for example, the ability to get more hardware in the event of a disaster.

You need an agreement with Dell or HP or anyone else to get the equipment and make sure that you have the capacity, power and other infrastructure to handle the data. For example, during 9/11, Merrill Lynch not only had backup of all its data and transactions, it had shadow trading floors already set up in New Jersey. When the exchange reopened, Merrill Lynch was trading. They were up and running even though they were in the South Tower when the airplane hit. We need redundancy in all the supporting infrastructure, not just the backup of the actual data.

It's interesting to look at Cantor Fitzgerald as well. They were the largest bond trader in the world, and they lost 657 employees on 9/11. A lot of people thought they'd never survive because it's a very relationship-based business. But from the IT perspective they were able to recover because all their data was backed up. Even with their infrastructure gone, they had Microsoft come in and recover their lost passwords and get their operating system back on line. A competitor let Cantor Fitzgerald use its systems while Texas Instruments rebuilt their infrastructure. They were able to recover because they had been backing up their data in real-time.

It's clear that IT-intensive companies like Cantor Fitzgerald and Merrill Lynch need a lot of redundancy and backup. But for other companies, it may not be as clear. How does a company decide how much redundancy it needs for its IT systems?

Any large company will need a minimum, such as daily backup. But then the question becomes, what happens if they lose one day's worth of transactions? For some companies it won't matter. It's not a company question though, it's a nature of the data question. At a university, for example, there are few items that need continuous backup. When they are doing financial transactions with a vendor, buying and selling supplies and equipment, they might need that backup. But other data, such as student information and research material, doesn't change that often; so if you do it nightly, it may be fine.

How should a CIO make a business case for their CFOs to invest in redundant IT systems? Do you have an example?

The more a CIO can tie redundancy to the regular business, the more chance he or she will get money for it. You'll need to go through what could happen if you go down in the same way you justify paying an insurance premium. You'll also want to look at it as an ongoing process of evaluating the risks you're facing. By building flexibility into any operation, you can respond better to market changes. The best way to do this is to build in redundancy that can help the business even before disaster strikes. For example, when you buy desktop computers, don't throw the old ones out—keep them as excess capacity. CIOs have to think about how to help the main vision of the business, which is to be profitable and increase the stock price. Having this redundancy on the IT side not only gives us insurance but also the flexibility to handle surges in demand when necessary.

OK, but what happens if you're really trying to cut costs in IT?

This is the big problem. Let's say you get prepared, and in the best of all worlds, nothing happens. The CEO asks, 'why are we wasting this money?' You've got to try to prove your point through benchmarking. It's hard to do because people don't get promoted based on cost avoidance. It doesn't show anywhere in the books. All managers, not just CIOs, face this. You can benchmark against leaders in the industry and present the consequences of not doing this. At the end, it's a management decision.

Are some people investing too much in redundancy?

No, because the pressure to cut costs is so intense that you don't see companies overdoing it. Individuals may overinsure and buy unnecessary warranties. But most corporations tend not to do it.

What's the best way to figure out the main risks for your company?

You want to have a brainstorm of all things that could go wrong and then plot them on a probability versus severity axis. Some events are very likely but don't threaten the survival of the company. For example, demand for a product is lower or higher than we thought or a truck has an accident. Some other potential disasters require more central planning, but aren't likely to happen, such as 9/11, Katrina or the Exxon Valdez oil spill, a strike, or a failure of the information system. All these things require the company to develop redundancy even if the probability is low. You'll have to plan for what you'll do because you'll also have fear among employees and customers, and the government may overreact. Even after 9/11, most of the economic damage came from the closing of our borders, not the actual attacks. Ford lost 13 percent of its fourth quarter production in 2001. They had convoys of trucks with parts coming from Canada and Mexico that couldn't get into the country. When foot and mouth disease hit in England, the government closed farms and culled livestock. To show they were in control, they also closed the countryside to tourists. Damage was 2.5 times larger to the tourism industry than to the agriculture industry.

The truth is, you're never sure you are prepared for the right thing. But if you build in some redundancy or flexibility, it doesn't matter if it's a hurricane, an earthquake or a strike. You'll be ready for anything regardless of the problem.

What's the one thing that's keeping CIOs up at night right now?

First of all, we are still in the era of IT viruses, which is an ongoing battle. Aside from that, IT and all the other functions are tied together. If the computers are down, the supply chain won't move. And if we can't buy the material [from suppliers], there is nothing to sell. Companies that do risk management well usually do it with cross-functional teams. In many cases the CIO is leading the group because the impact of losing IT infrastructure could be so severe.

But it goes beyond that. I just talked to Procter & Gamble, for example. Their Folgers plant in New Orleans got flooded after the hurricane. But their problem was not the plant—they knew how to get it up and running again. Their problem was they didn't have electricity, water or workers. So they dug a well to get water to the plant. And, in general, they have expanded the way they do risk profiles to include not only IT systems, which may go down, but also the support system outside of the plant. Companies have to expand the way they look at disaster planning and start looking beyond their own facilities to the greater ecosystem around them.

The truth is, you're never sure you are prepared for the right thing. But if you build in some redundancy or flexibility, it doesn't matter if it's a hurricane, an earthquake or a strike. You'll be ready for anything regardless of the problem.

Senior Writer Susannah Patton can be reached at spatton@cio.com.

Dated: March 01, 2006
http://www.cio.com/archive/030106/sheffi.html