CSO Fundamentals: The ABCs of Business Continuity and Disaster Recovery Planning

These days, the list of potentially business-disrupting events seems almost endless: viruses, power blackouts, natural disasters and even terrorist events. Good business continuity plans will keep your company up and running -- this primer helps make sure you've covered all the necessary bases.

Disaster recovery and business continuity planning are processes that help organizations prepare for disruptive events—whether an event might be a hurricane or simply a power outage caused by a backhoe in the parking lot. The CSO's involvement in this process can range from overseeing the plan, to providing input and support, to putting the plan into action during an emergency. This primer (compiled from articles in CSO magazine) explains the basic concepts of business continuity planning and also directs you to more CSO magazine resources on the topic.

Q: "Disaster recovery" seems pretty self-explanatory. Is there any difference between that and "business continuity planning"?

A: Disaster recovery is the process by which you resume business after a disruptive event. The event might be something huge—like an earthquake or the terrorist attacks on the World Trade Center—or something small, like malfunctioning software caused by a computer virus.

Given the human tendency to look on the bright side, many business executives are prone to ignoring "disaster recovery" because disaster seems an unlikely event. "Business continuity planning" suggests a more comprehensive approach to making sure you can keep making money. Often, the two terms are married under the acronym BC/DR. At any rate, DR and/or BC determines how a company will keep functioning after a disruptive event until its normal facilities are restored.

What do these plans include?

All BC/DR plans need to encompass how employees will communicate, where they will go and how they will keep doing their jobs. The details can vary greatly, depending on the size and scope of a company and the way it does business. For some businesses, issues such as supply chain logistics are most crucial and are the focus on the plan. For others, information technology may play a more pivotal role, and the BC/DR plan may have more of a focus on systems recovery. For example, the plan at one global manufacturing company would restore critical mainframes with vital data at a backup site within four to six days of a disruptive event, obtain a mobile PBX unit with 3,000 telephones within two days, recover the company's 1,000-plus LANs in order of business need, and set up a temporary call center for 100 agents at a nearby training facility.

But the critical point is that neither element can be ignored, and physical, IT and human resources plans cannot be developed in isolation from each other. At its heart, BC/DR is about constant communication. Business leaders and IT leaders should work together to determine what kind of plan is necessary and which systems and business units are most crucial to the company. Together, they should decide which people are responsible for declaring a disruptive event and mitigating its effects. Most importantly, the plan should establish a process for locating and communicating with employees after such an event. In a catastrophic event (Hurricane Katrina being a recent example), the plan will also need to take into account that many of those employees will have more pressing concerns than getting back to work.

Where do I start?

A good first step is a business impact analysis (BIA). This will identify the business's most crucial systems and processes and the effect an outage would have on the business. The greater the potential impact, the more money a company should spend to restore a system or process quickly. For instance, a stock trading company may decide to pay for completely redundant IT systems that would allow it to immediately start processing trades at another location. On the other hand, a manufacturing company may decide that it can wait 24 hours to resume shipping. A BIA will help companies set a restoration sequence to determine which parts of the business should be restored first.

Here are 10 absolute basics your plan should cover:
1. Develop and practice a contingency plan that includes a succession plan for your CEO.
2. Train backup employees to perform emergency tasks. The employees you count on to lead in an emergency will not always be available.
3. Determine offsite crisis meeting places for top executives.
4. Make sure that all employees—as well as executives—are involved in the exercises so that they get practice in responding to an emergency.
5. Make exercises realistic enough to tap into employees' emotions so that you can see how they'll react when the situation gets stressful.
6. Practice crisis communication with employees, customers and the outside world.
7. Invest in an alternate means of communication in case the phone networks go down.
8. Form partnerships with local emergency response groups—firefighters, police and EMTs—to establish a good working relationship. Let them become familiar with your company and site.
9. Evaluate your company's performance during each test, and work toward constant improvement. Continuity exercises should reveal weaknesses.
10. Test your continuity plan regularly to reveal and accommodate changes. Technology, personnel and facilities are in a constant state of flux at any company.

Hold it. Actual live-action tests would, themselves, be the "disruptive events." If I get enough people involved in writing and examining our plans, won't that be sufficient?

Let us give you an example of a company that thinks tabletops and paper simulations aren't enough. And why their experience suggests they're right.

When CIO Steve Yates joined USAA, a financial services company, business continuity exercises existed only on paper. Every year or so, top-level staffers would gather in a conference room to role-play; they would spend a day examining different scenarios, talking them out-discussing how they thought the procedures should be defined and how they thought people would respond to them.

Live exercises were confined to the company's technology assets. USAA would conduct periodic data recovery tests of different business units—like taking a piece of the life insurance department and recovering it from backup data.

Yates wondered if such passive exercises reflected reality. He also wondered if USAA's employees would really know how to follow such a plan in a real emergency. When Sept. 11 came along, Yates realized that the company had to do more. "Sept. 11 forced us to raise the bar on ourselves," says Yates.

Yates engaged outside consultants who suggested that the company build a second data center in the area as a backup. After weighing the costs and benefits of such a project, USAA initially concluded that it would be more efficient to rent space on the East Coast. But after the attack on the World Trade Center and Pentagon, when air traffic came to a halt, Yates knew it was foolhardy to have a data center so far away. Ironically, USAA was set to sign the lease contract the week of Sept. 11.

Instead, USAA built a center in Texas, only 200 miles away from its offices—close enough to drive to, but far enough away to pull power from a different grid and water from a different source. The company has also made plans to deploy critical employees to other office locations around the country.

Yates made site visits to companies such as FedEx, First Union, Merrill Lynch and Wachovia to hear about their approach to contingency planning. USAA also consulted with PR firm Fleishman-Hillard about how USAA, in a crisis situation, could communicate most effectively with its customers and employees.

Finally, Yates put together a series of large-scale business continuity exercises designed to test the performance of individual business units and the company at large in the event of wide-scale business disruption. When the company simulated a loss of the primary data center for its federal savings bank unit, Yates found that it was able to recover the systems, applications and all 19 of the third-party vendor connections. USAA also ran similar exercises with other business units.

For the main event, however, Yates wanted to test more than the company's technology procedures; he wanted to incorporate the most unpredictable element in any contingency planning exercise: the people.

USAA ultimately found that employees who walked through the simulation were in a position to observe flaws in the plans and offer suggestions. Furthermore, those who practice for emergency situations are less likely to panic and more likely to remember the plan.

Can you give me some examples of things companies have discovered through testing?

Some companies have discovered that while they back up their servers or data centers, they've overlooked backup plans for laptops. Many businesses fail to realize the importance of data stored locally on laptops. Because of their mobile nature, laptops can easily be lost or damaged. It doesn't take a catastrophic event to disrupt business if employees are carting critical or irreplaceable data around on
laptops.

One company reports that it is looking into buying MREs (meals ready-to-eat) from the company that sells them to the military. MREs have a long shelf life, and they don't take up much space. If employees are stuck at your facility for a long time, this could prove a worthwhile investment.

Mike Hager, former head of information security and disaster recovery for OppenhiemerFunds, says 9/11 brought issues like these to light. Many companies, he said, were able to recover data, but had no plans for alternative work places. The World Trade Center had provided more than 20 million square feet of office space, and after Sept. 11th there was only 10 million square feet of office space available in Manhattan. The issue of where employees go immediately after a disaster and where they will be housed during recovery should be addressed before something happens, not after.

USAA discovered that while it had designated a nearby relocation area, the setup process for computers and phones took nearly two hours. During that time, employees were left standing outside in the hot Texas sun. Seeing the plan in action raised several questions that hadn't been fully addressed before: Was there a safer place to put those employees in the interim? How should USAA determine if or when employees could be allowed back in the building? How would thousands of people access their vehicle if their car keys were still sitting on their desk? And was there an alternate transportation plan if the company needed to send employees home?

What are the top mistakes that companies make in disaster recovery?

Hager and other experts note the following pitfalls:

1. Inadequate planning: Have you identified all critical systems, and do you have detailed plans to recover them to the current day? (Everybody thinks they know what they have on their networks, but most people don't really know how many servers they have, or how they're configured, or what applications reside on them-what services were running, what version of software or operating systems they were using. Asset management tools claim to do the trick here, but they often fail to capture important details about software revisions and so on.

2. Failure to bring the business into the planning and testing of your recovery efforts.

3. Failure to gain support from senior-level managers. The largest problems here are:
   a. Not demonstrating the level of effort required for full recovery.
   b. Not conducting a business impact analysis and addressing all gaps in your recovery model.
   c. Not building adequate recovery plans that outline your recovery time objective, critical systems and applications, vital documents needed by the business, and business functions by building plans for operational activities to be continued after a disaster.
   d. Not having proper funding that will allow for a minimum of semiannual testing.

I still have a binder with our Y2K contingency plan. Will that work?

Absolutely not (unless your computers, employees and business priorities are exactly the same as they were in 1999). Plus, most Y2K plans cover only computer system-based failure. Potential physical calamities like blackouts, natural disasters or terrorist events bring additional issues to the table.

Can we outsource our contingency measures?

Disaster recovery services-offsite data storage, mobile phone units, remote workstations and the like-are often outsourced, simply because it makes more sense than purchasing extra equipment or space that may never be used. In the days after the Sept. 11 attacks, disaster recovery vendors restored systems and provided temporary office space, complete with telephones and Internet access for dozens of displaced companies.

What advice would you give to security executives who need to convince their CEO or board of the need for disaster recovery plans and capabilities? What arguments are most effective with an executive audience?

Hager advises chief security officers to address the need for disaster recovery through analysis and documentation of the potential financial losses. Work with your legal and financial departments to document the total losses per day that your company would face if you were not capable of quick recovery. By thoroughly reviewing your business continuance and disaster recovery plans, you can identify the gaps that may lead to a successful recovery. Remember: Disaster recovery and business continuance are nothing more than risk avoidance. Senior managers understand more clearly when you can demonstrate how much risk they are taking."

Hager also says that smaller companies have more (and cheaper) options for disaster recovery than bigger ones. For example, the data can be taken home at night. That's certainly a low-cost way to do offsite backup.

Some of this sounds like overkill for my company. Isn't it a bit much?
The elaborate machinations that USAA goes through in developing and testing its contingency plans might strike the average CSO (or CEO, anyway) as being over the top. And for some businesses, that’s absolutely true. After all, HazMat training and an evacuation plan for 20,000 employees is not a necessity for every company.

Like many security issues, continuity planning comes down to basic risk management: How much risk can your company tolerate, and how much is it willing to spend to mitigate various risks?

In planning for the unexpected, companies have to weigh the risk versus the cost of creating such a contingency plan. That’s a trade-off that Pete Hugdahl, USAA’s assistant vice president of security, frequently confronts. "It gets really difficult when the cost factor comes into play," he says. "Are we going to spend $100,000 to fence in the property? How do we know if it's worth it?"

And make no mistake-there is no absolute answer. Whether you spend the money or accept the risk is an executive decision, and it should be an informed decision. Half-hearted disaster recovery planning (in light of the 2005 hurricane season, 9/11, the Northeast blackout of 2003, and so on) is a failure to perform due diligence.

This document was compiled from articles published in CSO and CIO magazines. Contributing writers include Scott Berinato, Kathleen Carr, Daintry Duffy, Michael Goldberg, and Sarah Scalet. Send feedback to CSO Executive Editor Derek Slater at dslater@cxo.com.

Further Reading

More in-depth case studies in disaster recovery and business continuity planning:

Podcast: Anticipating Avian Flu http://www.csoonline.com/podcasts/cso_CarubisInterview_11082005.html

Restarting the US's Oil Engines http://www.csoonline.com/read/090105/restart.html

How can the oil and gas industry recover from a disaster as big as Katrina? With good planning, says Bobby Gillham, former CSO of ConocoPhillips.

Write People into the Plot http://www.csoonline.com/read/070105/write.html

Business continuity plans only work if they take employee needs into account.

Interview: The Optimistic Pessimist http://www.csoonline.com/read/020104/hager.html

Mike Hager escaped from the World Trade Center and got OppenheimerFunds up and running again in less than five hours. Now he faces another challenge: keeping America interested in business continuity planning.

Lessons from a Disaster http://www.csoonline.com/read/060103/briefing_lessons.html

Short and sweet, 10 things one practitioner learned after downtime caused by Nimda.


As one of the nation's largest insurance companies, USAA is in the business of managing risk. So it makes sense that-when faced with a disaster-the company knows how to respond.

CareGroup: All Systems Down http://www.cio.com/archive/021503/systems.html (from CIO)

Lessons learned from a major information systems outage.


In the weeks and months after 9/11, three CIOs working next door to the World Trade Center found they had to be strong leaders to get their companies back online. Now back in the city, they don't make business continuity plans. They live them.

Kodak: Weathering the Storm http://www.cio.com/archive/101500/weathering.html (from CIO Magazine)

Kodak's business continuity program addresses weather concerns and other threats.

2002-2006 CXO Media Inc. All rights reserved.

Reproduction in whole or in part without permission is prohibited.

Dated: May 01, 2006