



February 2004 – SC Magazine

## **Get prepared to avoid downtime**

by Marcia Savage

**Fires, power outages, cyberattacks. Natural and man-made disasters threaten every company, but in this increasingly internet-dependent economy, downtime and the losses caused by it are a major concern.**

Many companies are establishing business continuity plans (BCPs) to make sure they can recover if disaster strikes. Regulatory demands are adding to the pressure for business-continuity management, which is now no longer a luxury, but an expected part of doing business, says Jim Nelson, president of consulting firm Business Continuity Services, and lead instructor for DRI International (formerly the Disaster Recovery Institute).

"They're recognizing that they need to take pre-emptive, preventative steps to assure everyone associated with their organization they'll be here tomorrow, that they will be able to survive, whether it's a major event like someone crashing a plane into your building, or a virus or a cyberattack," says Nelson. "They're recognizing it's a lot more cost-effective to prepare prior to an event than to recover from a major incident." Major electrical blackouts over the past few years have reinforced the need for business-continuity preparedness, according to IDC, a market-research firm which expects worldwide spending on security and business continuity to top \$116 billion by 2007, growing twice as fast as IT spending.

Because outages in critical business systems or interruptions in service from key suppliers can have serious consequences, companies are doing more than establishing a separate data center for recovery purposes, according to market-research firm Gartner. In a September research note, Gartner analysts wrote: "Enterprises that employ best practices are incorporating business continuity management into their business process, application and technology architecture designs – and building in continuous 24x7 availability." Organizations have changed their approach business continuity, says Pat McAnally, senior director of marketing at SunGard Availability Services. When the disaster recovery industry was born in the 70s, the sole purpose was to recover data centers. "That's inside the glasshouse, that's where all the systems were. They didn't sit on people's desktops," she says.

"Then in the 90s, PCs were on everyone's desk and there were mobile sales forces with laptops. Now we had to worry about business continuity. It's outside the glasshouse. It's departmental servers, it's connectivity of users regardless of where they are. It's e-commerce solutions." These days, business continuity is morphing into information availability, explains McAnally. Service-level agreements are pushing companies to have information available more quickly than ever. "We find there's a tighter and tighter window for the amount of time you can be down," she says.



**However, in writing BCPs, many companies only consider what they should do in the event of certain scenarios, says Adam Lipson, president and CEO of consulting firm Network & Security Technologies. "A more sensible practice is to do a risk model. Not which servers or networks are critical, but which applications are critical to your business." Lipson states that once a company identifies its high-risk applications, it can plan a specific set of components needed for them, such as the type of data center and redundancy. "For the most part, business continuity is a reactive science. By taking a proactive role to business continuity, by overlaying a risk model on top of it, you have the opportunity to proactively address the problem," he concludes.**

Paul LaPorte, vice-president of marketing and business development at Evergreen Assurance, says that disaster recovery has traditionally involved recovery times of 24-72 hours. "For most mission-critical applications, that is long enough to seriously damage your business," he asserts. Increasingly, he adds, "CIOs will be judged on their ability to deliver dial-tone capability to their mission-critical systems." For the International Monetary Fund (IMF), making sure its email

system can be recovered quickly in the event of a network failure or outage is key, says Jack Roche, computer systems officer at the organization, which is based in Washington, D.C. After 9-11, the IMF embarked on formal BCP and determined that email was the most critical application to its staff of economists.

"They couldn't do without more than an hour's data loss. They wanted it up right away," recalls Roche.

IMF reviewed options for restoring its data center, such as contracting with a restoration site, but those took at least 24-36 hours, which didn't meet staff needs. It tapped Evergreen Assurance, which provides application-specific disaster recovery on a dedicated secondary site. If customers detect a problem or experience an outage, they press a button on a software console to automatically shift over to a secondary site, which has been continuously replicated. "We know in 15 or so minutes, with the push of a button, that we're able to failover all our mail services here in Washington, D.C.," explains Roche.

Uptime is also critical at Thomson ISI, an information solutions company that provides web-based data to researchers worldwide. "There has to be continuous uptime on these applications because they're used in all time zones around the world and because it's a fairly high priced database. We have contractual obligations to having a certain percentage of uptime and that's usually in the 99 percent category," says Jim McGhee, Thomson ISI lead systems engineer.

To ensure business continuity, the company uses F5's 3DNS Controller, which provides high availability and load balancing across distributed data centers. The product allows Thomson ISI, which has data centers around the world, to use DNS as a failover tool. "It allows us to do site-to-site failover if one of our hosting centers has hardware or power problems," says McGhee. "We can dynamically redirect traffic at a high level to another site".

As well as the pressures of meeting customers' high-availability demands, companies are also under regulatory pressure to implement business-continuity management.

"Never before in industry have we seen such a plethora of new regulations about business continuity and information security," says McAnally *Sarbanes-Oxley*, for example, requires every publicly-traded firm to have system controls that prove "beyond a shadow of a doubt" that its data is secure, reliable, available and compliant, she says.



Nelson says the corporate accountability mandated by Sarbanes, combined with an improving economy, drove increased interest in BCP in the second half of 2003.

Phil Bloodworth, partner and BCP leader at PricewaterhouseCoopers, also believes *Sarbanes* is the catalyst for a BCP resurgence. But it's driving a focused type of BCP, as opposed to taking an enterprise-wide view. "Through efforts largely driven by Sarbanes, that has led them to understand better in their organization where the risks are and where they have very specific needs for processes or a facility to be in place all the time," he says, "they're developing BCPs for these critical risk areas." Instead of BCP, the U.K. term "business-continuity management" is starting to be used more often in the U.S., says John Sharp, CEO of the Business Continuity Institute, a U.K.-based organization that supports the business continuity profession. "If you use business-continuity planning, the normal executive's approach is: 'Get me a plan written'," says Sharp. "But you can't do that, because it's an ongoing process.

Organizations change all the time, environments change, and it has to be something that you want everyone to be aware of, not just a plan on a shelf." Sharp advises that the first step in business-continuity management is to understand your business. "Not understanding the risks, because you never know what's going to come – 9-11 was an example of that – but knowing what it's going to cost you, both in terms of money and reputation, if you're unable to do a critical part of your business for any time." A company should consider its critical components against four P's – people, processes, premises and providers, adds Sharp, and rehearsing what needs to happen in the event of a disaster is crucial. "The first time you use it, you want it to work," he points out.

**However, in writing BCPs, many companies only consider what they should do in the event of certain scenarios, says Adam Lipson, president and CEO of consulting firm Network & Security Technologies. "A more sensible practice is to do a risk model. Not which servers or networks are critical, but which applications are critical to your business." Lipson states that once a company identifies its high-risk applications, it can plan a specific set of components needed for them, such as the type of data center and redundancy. "For the most part, business continuity is a reactive science. By taking a proactive role to business continuity, by overlaying a risk model on top of it, you have the opportunity to proactively address the problem," he concludes.**

McAnally says that information availability, keeping people and information connected all the time, needs to be designed right from the beginning. For example, a company putting in a new ERP system should review during the design process what it needs to keep its data secure, reliable and available. "It's easier to design that in at the front end than to do it retroactively," she says.

By establishing and maintaining a BCP, you will be ready for downtime – it is just part of the plan.