

Faced With New Challenges, BCP Continues to Evolve

http://www.securitiesindustry.com/reports/19_63/22935-1.html

Securities Industry News

October 27, 2008 By John Sandman

About a decade ago the primary business continuity planning (BCP) focus was Y2K, a global initiative with well-defined benchmarks and a hard deadline for systems migration. By contrast, the events of Sept. 11, 2001 saw lives and physical structures at risk as well as data and networks. Four years later the fires of 9-11 were replaced by the floods of Hurricane Katrina. And in 2006, BCP specialists turned their attention to a potential Avian flu pandemic.

Reacting to a multitude of threats and scenarios, BCP has had to expand its reach. "BCP professionals traditionally concentrated on making sure that the systems themselves are available," says J.R. Reagan, VP and managing director of global risk, compliance and security at consultancy BearingPoint. "Then they swung over to being process-oriented. The events themselves really run the gamut from events in nature, such as pandemics, to man-made crises like the current one on Wall Street."

In including the financial meltdown as a BCP issue, Reagan noted that the market is essentially staging an attack on itself. "What if my data isn't there anymore once a firm files for bankruptcy?" he says. "In the example of a firm asking for some of their collateral back from a counterparty, if, because the data's not available, they say, 'We'll get back to you,' that becomes ... at times a BCP problem." And without a solid business continuity program, he says, it can be impossible to tell whether or not a good-faith effort has been made to deliver.

Of course, "If anyone doing BCP a year ago said, 'Hey, let's plan for this,' I doubt if it would have been taken seriously," he adds.

As BCP evolves to tackle new problems, disaster recovery (DR) is increasingly viewed as a separate, interrelated discipline. "We look at DR as the process of recovering the systems," says Bob Guilbert, managing director of marketing at Eze Castle Integration, a Boston-based supplier of technology to hedge funds and other investment managers. "That can be as simple as a flooded data center, or even the blockage of access to the data center itself. BCP, on the other hand, is enterprisewide planning, looking at the people, processes and systems within the company."

Business continuity focuses on questions like "What are your business uses and critical processes? What needs to be in operation in the event that you do have a disaster?" says Guilbert, adding that firms must decide which aspects of their business are deemed mission-critical.

Eze Castle customers examine risk, "do a business attack analysis, write a plan, then train and test and provide ongoing maintenance," he says. "We treat BCP and DR as different aspects of that plan. We have clients that have disaster recovery but do not have a BCP plan."

While telecommuting, which has played a large role in plans for a pandemic, has emerged as a strategy, the electronicization of trading is far from the only reason, asserts Guilbert. "Independent of where the exchanges are, the ability to work anywhere gives the traders, hedge fund managers, portfolio managers and others the greatest flexibility," he says. "When you look at the way DR can be implemented, we choose an approach that is highly rigorous and highly focused on telecommuting." Guilbert recommends that firms employ hot sites--outsourced locations where desktops and other infrastructure can be located.

A drawback of such facilities is that their effectiveness diminishes when they are shared, as they often are. "If ten companies show up at a hot site that only has room for four, that's a problem," he says. "And some are oversubscribed."

The cost of preparedness has been climbing, according to Rodney Nelsestuen, research director for financial information services at Needham, Mass.-based TowerGroup. Before 9-11, "the cost was much lower because people thought that having things like taped backup for disaster recovery was sufficient," he says. "Post 9-11, people recognize that ... in the event of a fire, you'd not only lose your server, you'd lose your taped backup. You're now utilizing secondary data centers but have access in a quick timeframe."

How much a firm spends on disaster recovery depends on how often it's backing up information and how quickly it needs to recover. A company's recovery point objective (RPO) determines how much data will be saved. "If your backup is 24 hours ago, your recovery point will be data that's 24 hours old," says Guilbert. "If you are taking snapshots every hour, your recovery is every hour." The recovery time objective (RTO) measures how fast a firm can restore data. "If it's on tape, you need to find the tape, the place it's recovered to, and restore the data," notes Guilbert. "That could take minutes, hours, days."

In choosing a solution, a firm needs to "look at those two axes and determine what is the lowest cost of recovery time and recovery costs that I could accept," he observes. "Typically, it is very clear on the axes where your cost points are. The lower the RTO, the lower the RPO, the more expensive the solution."

TowerGroup's Nelsestuen notes that in terms of BCP, "what we have to respond to is not what we've come to expect in the past." Still, Nelsestuen favors a one-size-fits-all approach. "Even though the types of disasters and where they can occur seem to multiply, there are still only three basic ones: disaster caused by human behavior, disasters from natural causes and technical disasters," he says.

The real point of divergence, Nelsestuen says, is whether firms have tested their plans. Firms that he talks to all have plans in place, including for a pandemic, "but many of these institutions have not tested those plans very thoroughly. ... They haven't incorporated a lot of people across their business in that test. They might shut down the data center and start it up, or go to their off-site and do the disaster recovery part, but they don't try having their treasury department telecommute. And they need to."

Such exercises are disruptive, as shown by last year's industrywide pandemic test, sponsored by the Financial Services Sector Coordinating Council, Financial and Banking Information Infrastructure Committee and Securities Industry & Financial Markets Association. But even if such tests are "imperfect, getting people in the same room to talk about what they're doing and how they're doing it would be a big step forward," says Nelsestuen.