



December 2001/January 2002

VENDOR READINESS

By Susan Kelly

GMAC Mortgage Corp.'s treasury is located in Horsham, Pa., at a considerable distance from either New York City or Washington. But on Sept. 11, its cash management operations might as well have been located in lower Manhattan since the bank that handled its transactions was.

Overloaded phone lines even made it impossible to reach anyone in the bank's midtown offices, and the numbers that treasury managers found on the bank's Web site didn't lead to the people GMAC needed to talk to. GMAC's staff even tried calling Europe, but it was already too late in the day. Says Monica Estes, director of treasury services at GMAC Mortgage, "We really couldn't get hold of anyone."

So GMAC stopped sending through files, only to find out later that the bank which Estes declines to identify had successfully switched to its back-up system and was able to continue processing. The problem was that the mortgage company's officials had no way of determining that. GMAC was far from alone in its confusion. Corporations all over the world felt the impact of the deadly attacks just because one or more of their vendors and suppliers were located near Ground Zero, or had a vital facility in Manhattan, or lost key personnel. Companies nationwide were affected when the Canadian and Mexican borders were closed in the security crackdown that followed and when airports all across the U.S. suddenly shut down.

To review the state of preparedness of your own company in the wake of such a tragedy is the obvious first response. But as some executives learned during the drills for the ultimately utterly uneventful arrival of Y2K, the next question to ensure against business interruption must be: How prepared are the vendors and suppliers that provide a company's most valuable goods and services?

Perhaps surprisingly, despite the near-hysteria that surrounded Y2K, many corporations are still not in a position to evaluate the risks they face from potential disruption of their business-to-business networks. Here is a checklist of things to know about your vendor to make sure your company doesn't get into trouble because of another company's oversight or lack of oversight.

1. Know which services and suppliers are most important to your business. Then you must determine how long your company can operate if any of these are cut off and whether they are vital enough to merit enlisting an alternate provider. Companies need to assign a weighting system to functions, so they understand where they're willing to pay a premium, says Linda McLaughlin-Moore, senior vice president for treasury services and global clearing at J.P. Morgan Chase.
2. Ask your vendor or supplier what kind of back-up systems are in place for facilities, telecommunications and personnel. In this case, details count. So you must determine how old the plan is and when it was last tested. Many vendors can show you their disaster recovery plan, says Brian Turley, president of Strohl Systems, a business continuity software and consulting company in King of Prussia, Pa. It's a hard copy. It has an inch of dust on it. Obviously, that's not an executable plan. Ask not only what will be done, but how long it is expected to take. McLaughlin-Moore also suggests asking vendors about their past experiences recovering from disasters. Many times it will not only depict how well they do, but bring up other questions that the corporate might not have thought of otherwise, she says.
3. Find out whether executives at the supplier or vendor are familiar with emergency plans. Strohl's Turley suggests talking to members of the vendor's management team to be sure that they understand the plan and (that) it's an actual plan, not just something that is put in front of the customer. On Sept. 11 many companies found out how inadequately they had briefed various managers, he says. A lot of management team members actually worked contrary to what the plans had put in place.
4. Ask for a demonstration. Once the questions are posed, companies shouldn't be satisfied with mere words, consultants say. Absolutely, visit, says Donna Scott, research director at the Gartner Group. Vendors should be able to show you their business continuity plan. They should be able to tell you the last time or the last couple of times it was tested. They should be able to take you to the disaster recovery site, and show you the equipment and the workspaces.
5. Get an expert to evaluate the plans. Michael Redmond, senior manager in KMPG LLP's risk and advisory services practice, recommends that companies ask vendors to have their plans reviewed by a third party certified in business recovery



(page 2)

to be sure they meet standards set by groups like the Disaster Recovery Institute, the Business Recovery Institute and the Federal Financial Institutions Examinations Council.

6. Pay special attention to personnel preparedness. The one thing that most companies probably had not prepared as much for is the loss of people, says J.P. Morgan's McLaughlin-Moore. Some companies in the World Trade Center saw huge numbers of their employees die. Consultants note that all the back-up facilities and business continuity plans in the world are useless if there are no employees left to run the business. Corporates should be asking vendors whether employees are cross-trained or whether services are provided at more than one of the vendor's facilities.

7. Is your vendor prepared for the magnitude of physical destruction that took place on Sept. 11? Normally, when you create a plan, you assume at some point a day, three days, a week you can go back to your primary sites, Gartner's Scott says. For many companies, that wasn't the case because of the destruction in lower Manhattan. Thus, having relationships with real estate brokers becomes critical, she says, noting that while it took some companies days and even weeks to get back to business, others found alternate locations within hours or at least by the next day. It is also important for a vendor's back-up facilities not to be located too close to its primary operations. An alternate facility should be between 25 to 50 miles away and on different electrical and phone grids to ensure they're available during a disaster. Back-up facilities also should be accessible by different roads and modes of transportation. Turley, meanwhile, argues that the events of Sept. 11 suggest that a relocation facility ought to be in a different city entirely, since the destruction and clean-up operations made it impossible for many New York area employees to get to work anywhere in the metropolitan area. Yet, a back-up too far away necessitates an entire workforce be trained to run it.