

On Virus Alert

By Julie Segal

August 13, 2006

In the five years since 9/11, financial firms have learned that having backup centers for critical operations can be the difference between business life and death. But what if there were a crisis in which such centers were useless? What if employees were quarantined for long periods or were unable to travel to the home office or a backup center?

One such potentially disastrous situation would be an avian flu pandemic. The disease's potential for disruption is so great that two financial industry groups, the Bond Market Association and the Securities Industry Association, are considering creating a real-time centralized database of home telephone and e-mail addresses of employees at broker-dealers, investment firms, custodians, vendors and industry utilities so that financial sector employees could reach one another in the event they were forced to work from home for prolonged periods. Although backup systems typically furnish employees working from home with the electronic tools available in the office, such as trading systems, the database formed by the two trade groups would facilitate other kinds of communication, such as telephone conversations between custodians and money managers, which would be difficult to conduct if the participants were away from their offices and could not locate each other.

Joseph Sack, executive vice president of the BMA, which is expected to merge with the SIA later this year to form the Securities Industry and Financial Markets Association, says that although organizations have standing committees to address emergencies, a pandemic poses particular threats. As its effects would not be limited to one catastrophic day or even a week or two, a significant percentage of securities industry employees might be forced to work at home for long periods.

"The World Health Organization tells us that a pandemic would come in waves, possibly three months at a time, over an 18- to 24-month period," Sack says. "Our basic planning techniques may not be valuable in such a situation."

Technology firms have told the trade groups that the proposed database, which would include security and privacy measures, is feasible. All that's missing is the go-ahead, which Sack says may come after further discussion with firms, self-regulatory organizations, state and federal regulators and other government officials.

Gregory Ferris, managing director of global business continuity planning at Morgan Stanley and chairman of the SIA's business continuity planning committee, noted in testimony to Congress in late June that the danger in an avian flu pandemic is the likelihood that "employees in many different geographic areas would be affected simultaneously." He told legislators that given the possibility of commuting bans and school closures, "firms must understand how they can operate remotely, with the majority of employees working from home." This requires online capacity, and that capacity, Ferris cautioned, is only as good as a region's telecommunications infrastructure. He pointed to the December 2005 New York transit strike, which kept many area employees home and resulted in some slowed internet connections.

At a war game simulation conducted in January by the World Economic Forum and McLean, Virginia-based management consulting firm Booz Allen Hamilton in Davos, Switzerland, more than 30 senior industry and governmental executives concluded that if the flu arrived in Germany from Eastern Europe, the internet would be strained. "The backbone wouldn't be gone, but the edge of the network, where everyone was trying

to access their office from home, would be overwhelmed,” said participant William Thoet, a Booz Allen vice president.

At Lehman Brothers, Daniel Gonnella, co-manager of global business continuity management, has been preparing for a “denial of access” crisis by creating virtual workplace technology. Beyond being what he calls “an expensive insurance policy,” the technology is cost-justified because it enables employees to work from anywhere even if the flu doesn’t strike.

“And it familiarizes everyone with the technology,” he says. “If we built a big red tool box and put it in a corner to gather dust, then no one would know how to use it. If we use the tools every day, we don’t skip a beat.”

After 9/11, which forced Lehman to move from its headquarters at the World Financial Center, the firm implemented proprietary remote-access technology that allows employees using a remote PC to access the central office system. Recently, the firm has taken the next step, creating a solution that allows employees to access their office PC from any Internet connection.

Patrick Alesi, Gonnella’s co-manager, says that an operational industrywide directory would increase the number of traders and liquidity in a work-from-home system. “If you go to the ballpark with your glove and ball but there’s nobody else there, you can’t play,” Gonnella explains.

Boston-based Putnam Investments has provided employees with laptops and connected their homes with an encrypted virtual private network that is being upgraded for disaster recovery purposes. Philippe Bibi, chief technology officer at the firm, which manages \$180 billion in assets, says about 20 percent of Putnam’s workforce, or 600 people, already work from home and are able “to run trading applications without giving up anything, including recorded lines.” He notes that preparing for an outbreak of avian flu, however unlikely, “is like buying auto insurance; you regret not having it if you need it.”

At Wachovia Bank’s Evergreen Investments, which has almost \$251 billion in assets under management and offices throughout the hurricane-prone southeastern U.S., chief technology officer George Batejan has created a “buddy office” system in which an office is paired with another outside its region. Key applications are available at both. In addition, staffers keep office laptops at their homes and use the firm’s virtual private networks. Batejan says Evergreen recently implemented an automated call-tree system that contacts all employees in the event of an emergency to make sure that everyone is safe.

Smaller firms seeking to protect themselves, their employees and their customers are signing up for the services of third parties, says Chris Grandi, managing director of sales and marketing at Boston-based Eze Castle Integration, which provides outsourced information technology services. He notes that although 9/11 forced everyone to think about disaster recovery, many firms are only now starting to plan for broader catastrophes.

“Whether the problem stems from an outbreak of avian flu, a plumbing malfunction or an equipment meltdown due to air-conditioning outages, firms must plan for what to do if their primary office goes down or people are unable to get there,” he says. Grandi says that hedge funds, which for the most part do not have vast technological infrastructures, are being pushed into disaster planning by their institutional clients.

“I know of a number of hedge funds that won’t receive funding from these investors until they have presented proof of a disaster recovery plan,” says Grandi. Most of his firm’s solutions for hedge funds rely on virtual private networks and Citrix Systems’ Citrix, an application that gives users a view of their desktop as if they were in their office.