

## CONTINGENCY PLANS IN THE SPOTLIGHT

### Three experts discuss the increased importance of broad-based planning

**T**he Sept. 11 attacks demonstrated clearly—and tragically—that disaster-recovery planning is not a luxury, but a necessity in today's world. But it also highlighted flaws and weaknesses in many long-established plans. Partly, many experts said, because every disaster is different than the one before, and each is learning experience. In the case of the World Trade Center tragedy, one of the first lessons learned is that the scope of a disaster can be so large as to render existing plans moot. e-SECURITIES contributor Maria Trombly spoke to three disaster-recovery specialists. **Robert Cassiliano** is the president of Business Information Services, a technology services company headquartered near the site of the World Trade Center that is currently helping eight companies recover.

Cassiliano is also chairman of 7x24 Exchange, an association of facility and IT disaster-planning professionals. **Damian**

**Walch** is a senior vice president of continuity consulting for Comdisco, one of the largest disaster-recovery firms in the world, and a firm that provides backup operation sites for many Wall Street companies (SunGard Data Systems agreed to acquire Comdisco's continuity services business in early October). Comdisco is currently helping about 50 financial firms recover from the disaster. **Victor Mendes** is the CEO of Recall Corp., which



"The service providers have a six-week limit on the time you're allowed to stay at the recovery site... In this one there was no building to come back to. So don't assume... have a long-term plan."

—ROBERT CASSILIANO,  
BUSINESS INFORMATION SERVICES

collects daily data backup tapes for Wall Street clients and stores them at a location in New Jersey. Recall had eight clients in the World Trade Center, including Cantor Fitzgerald and Mizuho Financial.

**e-SECURITIES:** In terms of disaster recovery, what are the lessons that have come out of the World Trade Center attacks?

**Robert Cassiliano:** I see five distinct lessons. Number one is to

have some type of recovery plan in place. Even if it's an interim plan, it's better than nothing. For example, ABN Amro, in midtown, was relocating their trading floor. As an interim plan, even before they

contracted with a recovery-service provider, they kept the seats that they left behind cabled and ready. They're now using 100 of those to recover some futures trading that they had in the World Trade

Center. They could have dismantled those seats, but they had some focus on recovery and left those seats in place.

Number two: Ensure that your company has the ability to access information remotely. My company is an example of that. We're at 55 Broadway, about three blocks from Ground Zero and still can't get in the building [as of late September]. However, the building has emergency power so the technology is working. We are operating from our New Jersey office, and our technical people can get the information they need because we have remote access. It is possible that, although you can't enter the office, the technology might still be up and running.

Number three: A company needs to identify multiple staging areas or congregation points for people. Whenever you have a disaster-recovery plan, in the plan it said you're going to go meet at the Marriott across the street. What this disaster taught us is that the Marriott across the street might also be impacted by the disaster. You might need an alternate staging area out of harm's way.

Number four: This disaster, because of the widespread nature of it, and the number of firms and people that have been affected, teaches us a lesson that has not been seen before—don't assume that a recovery-service provider can accommodate your needs. They have different levels of how

they contract for recovery seats—some are shared seats, which are first-come, first-served, and some are dedicated seats, which are guaranteed. So if you're on a first-come, first-served basis, you might not get into a site. That has never happened before. On this one, although the service providers will tell you that they have not turned anyone away, they have scaled back some companies so much that those companies have been forced to find other accommodations and felt as though they've been turned away. So don't assume that a service provider can accommodate you with first-come, first-served seats. Contract for some percentage of the more expensive dedicated seats. Say, for example, if you need 100 seats, contract for 20 dedicated and 80 shared, so you are guaranteed to get at least 20 seats.

Number five: Don't assume that you can get back to your facility in six weeks. The service providers have a six-week limit on the time you're allowed to stay at the recovery site. And typically, if there's a power failure, fire or flood in your building, you leave for a week and you come back. This one, there was no building to come back to. So don't assume you can get back in six weeks; have a long-term plan.

**e-SECURITIES:** *What about at Comdisco? What lessons do you see?*

**Damian Walch:** The major thing that I would say we learned is, first of all, the importance of updated communi-

cations trees and lists to understand how people can be contacted, with primary and secondary contacts for both the critical people in your organization and the staff at large. Unfortunately, in this situation, there were so many people who were lost that it exacerbated the chaos—people couldn't be found and there had to be large groups of people just focused on tracking people down and ensuring their safety. One thing that we ourselves will do differently is create some mechanism for customers to better communicate with their employees and their field offices. The regular communication mechanisms were stressed quite a bit in the World Trade Center disaster. Second: There weren't primary, secondary and tertiary points for people to rally at after an outage, so people didn't know where to go after the outage occurred.

Third: People didn't have a clear understanding of roles and responsibilities. There may have been disaster-recovery teams and procedures, but the executives didn't understand who was responsible for what. Every executive and executive management team should understand their roles for damage assessment of the site, public relations and so on. Fourth: The executive management team should clearly understand what is done for data backups in an outage like this. Typically, executives aren't concerned about things like this, but they should ask these questions—what happens if we lose these systems, what happens if we lose this data? Fifth: Plan for complete

processes, not just data. Most businesses and most environments are dependent on applications and in order to get to those applications you may go through a local server of some kind or a router and once you connect to the data center you may go through a firewall and authorization services. Somebody absolutely has to look at how end-users connect to the system and architect that solution or it will increase your recovery time. You'll have to acquire equipment in some cases, reengineer networks and recreate that information flow. You could also potentially lose critical data that resides on one of the components in the information flow.

Sixth: Test with the actual people who'll be doing the recovery. What tends to happen in companies is that they do the test with people that are available at the time of the test, vs. the people who would actually go through the recovery process. Seventh: There were a lot of companies that were simply undersubscribed to their [backup] environment. Almost everyone underestimated the number of seats that they would need to come up to business.

**e-SECURITIES:** *How many of your clients needed to use the recovery services after the disaster?*

**Walch:** The total number we've recovered is 47, with 92 disaster declarations. What that means is some of those 47 companies might have had multiple platforms that they subscribed to. We also had four disasters that were not included in that num-

ber that occurred in the United Kingdom—two that could be attributed to the World Trade Center activity and two unrelated. We had two companies that had major offices in the World Trade Center and they declared a disaster in the United Kingdom and moved traders into those facilities to handle overflow or customer calls. This is a record for us. The closest we had before was during Hurricane Floyd, with 26 concurrent disaster declarations.

**e-SECURITIES:** *Tell us about your facilities.*

**Walch:** In the New York Area, we have three total—in Queens and New Jersey. The Queens facility, in Long Island City, has 100,000 square feet of area. The North Bergen facility has 163,000 square feet. The Carlstad facility has 302,000 square feet. There's also a facility in King of Prussia, Pa., and one in Columbia, Md. There are 3,000 people in those three facilities in the New Jersey and New York area, with 300 seats still available. We have about 400 seats left in the two locations in Pennsylvania and Maryland.

**e-SECURITIES:** *Do the recovery facilities just have trading seats or backup data as well?*

**Walch:** We don't do offsite storage of data, like an Iron Mountain would. But we absolutely will do mirrored or replicated data in an alternate facility. We actually manage about 50 customers' data in that fashion, where we back up their data in an alternate location.

**e-SECURITIES:** *Will Comdisco do anything differently in the future because of Sept. 11?*

**Walch:** The one thing that we will do differently is we will develop approaches for customers to better communicate with their employees and their field offices. We'll try to create some mechanism for regular communications, which were stressed quite a bit in the World Trade Center disaster.

**e-SECURITIES:** *What lessons did Recall Corp. learn from the World Trade Center disaster?*

**Victor Mendes:** If there's a lesson for us at Recall it's that we have to be more emphatic with our own customers about the importance of keeping their contingency plans up to date. Sometimes, circumstances change. Different sites are brought up as alternate sites, volumes of information change, and the plan that was put together just a year ago may not be totally up to date. Further, there must be an ongoing commitment to contingency planning. You need to consider in your contingency plan how much data you can afford to lose. If you lose a day's worth of operations, are you going to be OK? Perhaps if you're a small company. If you can't lose a day's worth of data, can you lose half a day or three hours? Some companies had this as an objective, but as a cost-cutting measure had been gradually reducing the number of daily collections. In times of tranquility, this appears to be a place where you can save some

money. So they didn't have what they thought they should have when it came time to recover their data.

Also there's a general need to think about the paperwork. When you look at every picture of the destruction, you find so much paper all over the place, so many documents, everything that was in-process. Some companies actually had contingency plans that were written in paper form. All the paper that was used by those companies is gone. That could have been avoided if companies were using imaging technologies to keep those documents stored in digital form. Then they would have had electronic access to those documents, and it's a more effective way of working with documents instead of moving paper around.

**e-SECURITIES:** *Tell us about your facilities.*

**Mendes:** We have two sites—two media vaults, or data protection centers, that serve this area. One is located in New Jersey, within 10 minutes of the financial center, but on the Jersey side. We have about a million backup tapes that we keep for almost 700 customers in the area. We're continuously rotating these tapes—these are not

static tapes, these are tapes that contain the latest information. All tapes are rotated about once a month. If it's been sitting in the media vault for about a month, it's time to be sent back to the company to be rewritten with the latest information. Then there are some archival tapes that are kept permanently. We go to the customers and pick up new tapes on a daily basis. We have about 35 drivers and vehicles continuously circulating around New York.

**e-SECURITIES:** *Were any of your drivers in the World Trade Center at time of the disaster?*

**Mendes:** Fortunately, all of them were accounted for. We contacted them very quickly—they all have cell phones, and within a couple of hours, we accounted for all of them. The first delivery in the World Trade Center was scheduled for 10 a.m., so fortunately, they were not close enough to the place then to be impacted.

**e-SECURITIES:** *When are the backup tapes used?*

**Mendes:** In the course of business it is often the case that a file is corrupted or a virus infected a particular set

of files and we're called in an emergency basis just to bring in a few tapes or a set of tapes to do a partial recovery of some files. On a larger scale, when it's a disaster that we had, it's a much bigger operation. We're called to trigger a disaster-recovery plan—it's a fairly elaborate process. There's a disciplined contingency plan that a company has to produce and we guide them, help them with the planning. They need to know, for example, who is authorized to declare a disaster. There's a chain of custody—if this person isn't available, this other person will do it. Then, what are the locations that are ready to receive backup tapes? These are either alternate sites that run with low capacity or on standby, or they have contracts with companies that keep those places ready to receive data. We quickly assemble all the tape sets that a customer will require and transport them as quickly as possible and deliver them to their specified location. In our case, we had about 20 declarations within a couple of days following the strikes—mostly Wednesday and a bit Thursday. We had all of these tapes delivered on time to the customers that requested them, including Cantor Fitzgerald.

---

Reprinted from *Securities Industry News*, October/November 2001. 11 Penn Plaza, 17th Floor, New York, NY 10001, (212)631-1516

---



[www.bizinfoservices.com](http://www.bizinfoservices.com)