The Problem with How Most People Test Their Recovery Capability

JOHN JACKSON

This article isn't so much about a trend or direction in our industry as it is about one of the most serious problems I have seen over the years — the lack of realism in testing recovery programs.

Reflecting on my 20-plus years with Comdisco, SunGard, and IBM, I have participated directly in, overseen, or audited hundreds if not thousands of tests for customers — including those many of you reading this article have conducted. Combine that with the tens of thousands of tests vendors have supported, and there is a tremendous base of information on the approach to testing and the success people have.

The most relevant fact, however, is what happens when people declare disasters — the true test of how effective the testing programs are. One key point stands above all: In all of the tests I have witnessed, 100 percent of the time the recovery configuration didn't match the production environment that was being recovered. You might find that astonishing, but it's not when you consider how people test.

Prep Time

Now we all know that most disasters, whether affecting IT facilities or business units, come with little warning. Certainly hurricanes are a slight exception, since technology today at least gives us some warning, but you should agree that most disasters come with little preparation time. So let's think about how most people test. I'm not talking about the first one or two tests, but rather the ongoing process of testing.

Considering the lack of warning or preparation time in a real event, let's look at a typical testing scenario. Companies usually start planning their tests about six months before the actual event is to take place. Some have shorter prep times, some longer, but let's use six months for this discussion. Two primary reasons for the long schedule time — the difficulty in securing test time (which might be another article in itself) and the prep time most people and vendors allocate.

So we get the team together and start discussing the test objectives and timeframe. We contact the vendor and secure our test time, so we know we have access to the center. Next, we inform the staff of the test dates, making sure people will be available, allowing for vacations, holidays, and any other known conflicts. Along the way, we discuss the test plan, laying out the time frames, roles, and responsibilities. We tell everyone when they need to show up, we book hotel rooms, we book flights so we get the best airfares, we book cars — everything geared towards making the test go as smoothly as possible. See any problems yet?

Next, we determine exactly which data we will need to test the applications. We back it up several days before the test and ship it to the recovery center so the vendor can unpack the tapes and inventory them; or we create a copy of our replicated data so we have it ready to go. We certainly don't want missing or corrupt data to impact our test.

Finally, the test date arrives. We get to the center the day before, get a good night's sleep, double check our plans and most often have a "successful" test. The test may have met criteria for success, but it the manner in which it was conducted was an unrealistic view of what happens in real-world situations — and isn't that exactly what testing should prepare you for?

Organized Chaos

Now I am not saying this process is not with its virtues — certainly going through the test process in this fashion has its good points and does ensure the team understands the process. But, in my opinion, these tests don't reflect the reality of a disaster. When the real event occurs, there is no time to prep, no advanced airfares, hotel rooms, or rental cars. There's no ability to back up the data; you must rely upon what's stored offsite (hopefully), and there's no time to rest before recovering.

Testing needs to be organized and chaotic, planned and unplanned, to ensure we *really* know how successful the recovery will be. It also needs to put some stress on the configuration at the recovery site — whether systems or PCs — to see if the capacity and performance is adequate to actually get the job done, not just make sure things work.

So my recommendation is to develop a comprehensive testing program, one that mixes planned, scripted tests with unplanned, reactionary tests that stress the process, the people, the data, and the equipment. This combination most certainly will cause some "failed" tests,

but that is exactly what you should hope for — tests that find problems so you can fix them before it's too late.

Also, the test planning process is a terrific time to match your recovery configuration against your production configuration and see if changes in production are properly reflected. I have witnessed customers declaring and saying, "What do you mean I still have a mainframe contract? We got rid of our mainframe months ago!" You probably would say that couldn't happen, but trust me it has. And it can happen to you if you don't keep things in sync.

Keep It Real

Last but not least — and you may really be surprised by this one — test your actual recovery plan, not your test plans. Remarkably, many companies never actually test the plan itself. They test all of the components, but not the plan that they intend to follow when a disaster occurs. How do I know this? By seeing company after company come to test without their recovery plan.

Involve your actual plan in the whole process of scheduling, preparing for, and conducting your test. Use the declaration process in your plan to schedule the test. See if your plan allows for booking hotel rooms, cars, and airline tickets. Validate your plan's timeline against your test results to see if your planned recovery times can be met.

Bottom line: Use your tests to make sure you can recover, not just to get a nice check mark from your auditors. **CI**

John Jackson is a co-founder of Fusion Risk Management and a member of the Continuity Insights Editorial Advisory Board. He is an expert in the fields of business continuity, disaster recovery, and high availability. His 30 years of experience includes running all aspects of IBM, HP, and Comdisco's disaster recovery businesses and participating in over 500 actual recoveries for client companies. He can be contacted via e-mail at JJ@FusionRiskMgmt.com.

Ad Index