information security matters

Do You Need a Disaster Recovery Plan...?

It is those three dots that save me from accusations of rank lunacy. (Oh, well, from accusations based on this subject.) What follows the dots is "as disaster recovery moves into the cloud." Even more specifically, I am speaking of utilization of Disaster Recovery as a Service (DRaaS), the commercial relationship in which a third-party company receives and stores replicated and backed-up data and provides servers for testing disaster recovery with an expanded number of them in an actual disaster. Most critically, a DRaaS provider carries out the recovery when requested, according to specified service level agreements (SLAs). A business can, therefore, buy (rent, really) recoverability in one-hour, four-hour, one-day increments or at whatever service levels a given vendor is willing to offer.

The Advantages of DRaaS

DRaaS offers a number of advantages over the use of commercial hot sites or internal recovery data centers. It relieves organizations of the sudden need for a larger cadre of technical personnel at a time of crisis. It simplifies disaster recovery testing from an annual techie trek to a recovery site for a weekend of work and turns it into a phone call, followed by waiting for results. It must be mentioned that that phone call triggers action on the DRaaS vendor's end and, thus, possibly an invoice thereafter. DRaaS is a force multiplier at a time when many organizations are outsourcing technical work to other regions of the globe; those overseas workers might not even be able to access the recovery environment, much less recover systems there. Finally, in an era in which much production processing is being shifted to the cloud, it just makes sense to move recovery there as well.

But that raises the question alluded to in the title of this article: If a vendor is doing the work of recovery, with SLAs (think recovery time objectives and recovery point objectives) established by contract, is there a need for an organization to have a disaster recovery plan (DRP) at all? I can see three potential answers, and every time I think I have decided on one, the other two come roaring back to undermine my confidence.

No, You Do Not Need a Plan

Why buy a dog and bark yourself?

Engaging in a relationship with a DRaaS vendor means assigning to that company the responsibility for recovering the buyer's systems. Implicitly, the vendor asserts that it knows how to carry out its contractual obligations and that can be proven (or disproven) by testing. Perhaps the organization acquiring DRaaS support had detailed procedures for how it was going to recover X, Y and Z systems from Point A to Point B. Those plans become irrelevant when the very paradigm of system recoverability is overturned. I am hardly the first to note that the cloud changes everything.

Moreover, the acquiring organization has no say in what the system recovery procedures might be. Those are the trade secrets of the vendor. It may feel like an awful waste to lose the accumulated knowledge of decades of disaster recovery planning

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

Steven J. Ross, CISA, CISSP, MBCP
Is executive principal of Risk Masters International LLC. Ross has been writing one of the *Journal*'s most popular columns since 1998. He can be reached at stross@riskmastersintl.com.

and that may cause the loss of a job or two. But they say that is what disruptive technology is all about. That accumulated knowledge is inside heads with fewer, but grayer, hairs on them. What is the point of passing it on, except as an historical artifact? We once lost an awful lot of COBOL expertise and got along quite well without it.[1]

Oh, yes, there is still the need for a plan containing contact information for the DRaaS vendor, a process maintaining currency between production and recovery systems, and procedures for validating recovered systems and data. But that is hardly what we mean by a DRP.

Yes, You Need a Plan, but Not as Much

Or maybe that is what we mean.

Another unoriginal observation—I got a million of 'em—is that you can outsource responsibility, but not accountability. Therefore, the organization obtaining DRaaS support must extensively document how it will execute its accountable activities. These will include all the same preliminary steps that an internal DRP should contain, including the determination that an IT-related disaster has occurred; how to declare it *vis-à-vis* the DRaaS provider, oversight of the recovery processes and communication with organizational stakeholders while recovery is underway.

Perhaps the most important part of a DRaaS-based DRP is to document an understanding of how the organization will conduct business while systems are being run remotely. Inevitably, there will be differences between business as usual and the DRaaS-supported period. Revised operating procedures should be thought through and documented before they are needed in order to avoid painful fumbling at precisely the worst possible moment.

Finally, the DRP needs a section on how to restore normal operations once the disaster is over. If that means a return to an organization's own data center, this will be tricky. DRaaS vendors are a fount of guidance on how to transfer processing to them, but they are not as good at telling customers how to go the other way. If an organization is using the cloud for software and/or infrastructure as a service (SaaS/IaaS), it is trickier still, since that vendor is now responsible for its own recovery, taking matters away from the buyer at one remove even further.

"The most important part of a DRaaS-based DRP is to document an understanding of how the organization will conduct business while systems are being run remotely."

Yes, You Need a Plan at the Same Level

All the foregoing assumes that the DRaaS vendor itself will not fail, with several meanings to the word. It applies to a vendor that fails to provide adequate service, fails to recover within the SLAs, or, at worst, just fails and goes out of business. The organization that buys DRaaS needs to consider these eventualities at the time of acquisition. Think of it as a prenuptial agreement that an organization makes with itself, because the DRaaS vendor will certainly not be involved. Perhaps a sort of "living will" can be included in the contract, but again, the vendor has little incentive to go along with this.

This leaves the acquiring organization with the odd responsibility to plan for recovery from a production environment that faces a potential disaster to a data center that does not exist. With recovery

planned for DRaaS, the buyer must provisionally accept future failure and plan for it. This is not only counterintuitive, it is very difficult to fund and impossible to test. It might deter the decision to use DRaaS, but once that decision has been made, the "what if" thinking should begin.

Where do I come down on all this? As I said at the outset, I am of mixed minds on the matter. There is a certain whack-a-mole[2] quality to the whole subject. If pushed to the wall, I would say that organizations need to have their own plans for what they would do while the DRaaS vendor is doing what it does. I would not tell a mechanic how to fix my car, but I would plan for what I would do while the car is in the shop. That is an inexact analogy, but it is the best I have for this column.

Endnotes

1 Except in the lead-up to the Year 2000.
2 There was an American arcade game in the 1970s, for those who do not remember America in the 1970s, in which moles would pop up from one hole and, when banged back, another would pop up somewhere else. The term is used for the practice of repeatedly getting rid of something, only to have more of that thing appear, such as deleting spammers' email accounts or closing pop-up windows in a web browser. In other words, it is "on the other hand and on yet another other hand" in colloquial slang. *http://onlineslangdictionary.com/meaning-definition-of/whack-a-mole*