Disaster Recovery Management in the Multi-Modal Era

Multi-modality in IT environments implies complexity. The concept of an organization's information systems operating in a space and on equipment owned by that organization has been replaced by systems residing in:

- A proprietary, "in-house" data center
- A commercial colocation (colo) site
- An outsourced data center
- A managed services provider
- A remote, vendor-operated site, providing a service over the Internet
- The cloud, a commonly used term for a series of commercial data centers in which a customer executes its applications or acquires commercial services

Oh, by the way, all at the same time.

This complexity is difficult to manage even in the best of times. Having a disaster strike any of these venues is decidedly not the best of times. (Others wiser than I can decide whether a physical disaster is the worst case or if that "honor" belongs to being the victim of a destructive cyberattack.) I think that I speak for all of us in saying disasters are pretty bad and ought to be avoided.

Geographic Diversity

Multi-modality is, in part, a response to the threat of disasters. Its very structure ensures that a single disaster does not wipe out everything, just that portion of an organization's systems unfortunate enough to be located where a disaster hits. Or am I being too free with the word "ensures"?

One of the factors that should influence decisions about moving a system out of a proprietary data center is where it will then be located—beyond what it can do, how it is secured and how it performs. If the intent is to reduce risk, then moving systems to a colo across the street from the organization's headquarters and to an outsourcing provider next door will not accomplish very much. As ever, poor design can undermine the best of controls and security features. The word "ensures" should be replaced with "enables"; it is up to system architects to provide assurance that a multi-modal environment contains sufficient geographic diversity to meet its overall disaster recovery objectives.

Proprietary Data Centers

Even in a multi-modal architecture, there is still a need for a proprietary data center.[1] It is the central point for communicating with all the systems elsewhere. It also houses computers driving building management and access control systems, as well as Internet of Things (IoT)[2] equipment, around the building.

Planning for recovery from a disaster at an "in-house" data center is actually more difficult now than previously. In the old days (oh, about a decade ago), most of an organization's applications and infrastructure resided in its own data center.

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.

http://bit.ly/2rTqwSL

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.

Therefore, planning for a disaster in that location required having a second data center somewhere else, far enough away that the same disaster would not incapacitate both.

Now, simply finding another place to run these systems is insufficient, perhaps unavailing. If they could have been transferred out of the data center, they would already have been, in the move to multi-modalism. What would be the point of a remote telecommunications termination hub if a building's demarc is destroyed? Even if a remote link could be established, how would data be delivered to the desktop? How would the phones ring?

Colo Sites and Outsourcers

Use of a colo site often has more to do with mechanical, electrical and plumbing (MEP) issues than IT. For many organizations, the economics of powering and cooling a data center just do not make sense if those burdens can be transferred to a third party. For others, migrating from an organization's own data center to a colo is simply a transitional phase on the way to Anything as a Service (XaaS).[3] Whatever it is, the decision to move servers, storage and telecommunications into a colo means moving them into not one, but two sites: a prime and a backup. An organization may already have a disaster recovery facility and it may serve for the transferred systems, or maybe not. Testing is in order before total reliance is placed on the colo-based systems. The same point can be made about outsourcing[4] one or more applications and their associated infrastructure. In choosing an outsourcer, it is incumbent on the customer to ensure that that hosting company has at least a second data center, as well as a well-tested and maintained plan for using it if the time should ever come. The basic premise of dual data centers is still in force.

Managed Services and Software as a Service

A special case of outsourcing is managed services: in essence, hiring someone else (a managed services provider [MSP]) to do work that an organization does not want to or cannot do itself. These include certain IT functions, particularly email hosting, performance management, security monitoring, storage, backup and recovery, and network monitoring.[5] Of course, many of these activities can be done anywhere an MSP decides, but some require hands-on work. So, buyers should consider how these services will be provided if there is a disaster wherever the systems and, even more important, the workers happen to be.

> "A TRUE CLOUD IS A SUPERB SOLUTION TO DISASTER RECOVERY PROBLEMS."

The need for due diligence is greater in the case of Software as a Service (SaaS) accessed by a customer over the Internet.[6] An organization has the use of software, typically on a subscription basis, but does not own that software nor the servers and storage on which it runs. That equipment is somewhere and, in preparing for recovery from disasters, has to be somewhere else as well. Where that "somewhere" is matters, as does the frequency with which the software and customer data are replicated from place to place. These are not novel considerations, but many SaaS subscriptions are made by business functions, not IT, and disaster recovery may be overlooked.

The Cloud

A true cloud is a superb solution to disaster recovery problems. Note the modifier "true." There are vendors claiming to offer cloud services, but a little investigation will show that they are just hosting services with a few sites. They do not offer the underlying infrastructure and mechanics of a true cloud, in which the same software (usually virtualized) runs simultaneously in two or more locations, with data replicated at frequent intervals among them. The intent, and in many cases the actuality, is that operations can be switched from

site to site with little or no impact on the customers. This may be done for performance reasons, load balancing or recovery. With attention to the latter, it is essential to verify the infrastructure claims of the salesperson and validate that this automatic failover actually works before committing to a cloud provider.

In this era of multi-modal technology, many disaster recovery issues are solved, some are simply transferred and a few are made worse. Disaster recovery is manageable, but only with one's eyes open.

Endnotes

1 This assumes that an organization has a building where its people work, which is only partially true today. Many people work remotely some or all of the time. The future may lead companies and government agencies to divorce work from real estate and the residual data center may actually disappear.

2 Addressed in Ross, Steven J.; "The End of the Beginning?" *ISACA® Journal,* vol.3, 2017, *http://www.isaca.org/Journal/archives/Pages/default.aspx*

3 McLellan, C.; "XaaS: Why 'Everything' Is Now a Service," *ZDNet*, 1 November 2017, *www.zdnet.com/article/xaas-why-everything-is-now-a-service/*. Pronounced zăss, it means "Anything as a Service."

4 In using a colo, an organization owns the equipment and rents the floor space and MEP. If a system is outsourced, the organization owns the application(s), but not the equipment on which it runs, nor the floor space, nor the MEP. These are subtle differences, to be sure, but crucial in planning for disaster recovery.

5 Olavsrud, T.; "How to Get the Most From a Managed IT Services Provider," *CIO*, 30 June 2017, *https://www.cio.com/article/2930498/it-strategy/why-businesses-are-turning-to-managed-it-services.html*

6 Hufford, J.; "Cloud Vs SaaS: What's the Difference?" *nChannel*, 13 July 2016, *https://www.nchannel.com/blog/cloud-vs-saas/*. All such services based on software in a cloud are SaaS, but SaaS need not be in the cloud. The services can be accessed directly without passing through a cloud provider. This is a source of confusion and some controversy, into which I do not intend to enter here.