Managing Availability in the Multi-Modal Era

2018 marks the 20th year of Steven Ross' Information Security Matters column in the *ISACA® Journal*. This column has remained one of the most popular columns in the *ISACA Journal* through the years. ISACA® is deeply grateful to Steve for his time, his expertise and his talent as an author and a valued colleague. The *ISACA Journal* editorial team looks forward to many more years of successful collaboration with Steve.

A few columns back, I wrote about the security of multi-modal IT environments,[1] in which applications and infrastructure are operated in colocation (colo) sites, as Internet-based services; in the cloud, as managed services; and in proprietary data centers—all at the same time. In that article, I dropped a rather heavy hint that I would address disaster recovery in multi-modal environments and I will do that, but I would like to expand a bit on availability management first. Nothing has changed regarding multi-modal availability management. When something stops working, it has to be fixed and brought back up. Nothing has changed…except so much is different.

Finding Fault

Outages may be caused one of two[2] ways: by logical failure of data, software or infrastructure, or by physical disruption (i.e., a disaster) affecting equipment or networks. When a system or many systems go down, it is not always immediately evident where the cause lies. Thus, when systems flatline, the first task for IT operations personnel is simply to find out what happened and where. When all systems were operated in a single data center on an organization's own premises, this was relatively simple. With those systems in many locations, figuring out what is going wrong is considerably more difficult.

Organizations with more than one data center already face this problem, but at least those organizations own all the sites. Things get more complicated when multiple owners are involved. If, for example, a department uses an Internet-based service, an outage might be traced to an organization's own data center, to its

telecommunications carrier(s), to the servicer's data center(s) or to its carriers. In the immediate aftermath of an outage, it is often the case that the people responsible for each are also trying to figure out what is wrong. Until who is at fault can be established, each one blames all the others.

The Virtual Console

Managing availability in a multi-modal environment is challenged by the relative obscurity of all the components in that environment. This raises the importance of a virtual console[3] that enables visibility into all of an organization's systems, wherever they may be or regardless of who owns them. When one component fails, that might be a stand-alone event or it might have a knock-on effect on other components. For example,

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.

a cloud-based application might generate data that are used by another application running in a colo data center. Without a virtual console that enables an organization to see and to manage both simultaneously, there is a high likelihood of downstream problems. And, if both cannot be recovered to a common point in a concerted manner, those problems may be reflected in an overall loss of control over the data.

> " WHEN AN ORGANIZATION MOVES DATA AND SOFTWARE TO A COLO, IT LOSES CUSTODY BUT RETAINS AGENCY. "

Or is "loss of control" the correct phrase? To a great extent, organizations that institute multi-modal architectures[4] have already lost a degree of control over information resources and, thus, over the availability of those resources. When an organization moves data and software to a colo, it loses custody but retains agency. In the case of managed services, it may keep custody, but lose the ability to initiate, execute and control its resources. Thus, the *availability* of data (and the recovery of access to the data when access is interrupted) must be distinguished from the *use* of the data and their recovery following an outage. Where an organization runs its own data center, it is responsible for the availability of both data and software in the event of a disruption. This may not be the case when some or all of custody and use are given to third parties. All of which is a convoluted way of saying that managing availability in a multi-modal environment is quite complicated.

Responsibility and Accountability

Note that I said *responsibility* for availability. Responsibility can be assigned, but *accountability* for availability remains with the owner of the relevant resources. In some ways, this is just another case of the ongoing discussion of control over outsourcing.[5] Simply put, the owner of a resource is accountable for its availability even if it has chosen to "hire" someone else to carry out the tasks involved. The distinction only seems to be an issue in organizations where the prevalent culture leads to retention of ownership along with evasion of responsibility.[6] When contemplating a multi-modal architecture, organizations must consider both maintaining the availability of information resources as well as which entities will have the access and the tools to provide availability.

This seems confounding only because we view the whole range of making information resources available—ownership, accountability, responsibility, access, recovery, security, operations, *et al*—from the perspective of IT-the-way-it-used-to-be. An apt analogy might be houses-the-way-they-used-to-be. A few centuries ago, as the pioneers spread across the plains,[7] if you wanted a house, you built it. You owned it and the land beneath it, too, by dint of the fact that you had built a house on it. If you wanted heat in your house, you chopped down some trees. If you wanted food, you grew it or killed it. If you wanted water, you dug a well. If you wanted your house to be there when you went away, well, you did not go away very often. Today, most of us have "outsourced" our heat, food and water. We may own our houses, or we may have occupancy, but not ownership of either the house or the land (i.e., rentals).

We understand that the responsibility and accountability for continued existence of houses are shared explicitly by the owner and the occupant, who may or may not be the same. The lines of demarcation are established in contracts and laws. The same is true of IT in a multi-modal environment. What, after all, is a service level agreement (SLA)

in an IT contract but a commitment by one party to make information resources available and by the other to accept limited periods in which they are not? Managing availability in a multi-modal environment requires a great deal of attention to details, which are being defined by the multi-modal pioneers of our day. Perhaps we are all pioneers now, but we will become settlers someday.

Endnotes

1 Ross, S.; "Information Security in the Multi-Modal Era," *ISACA® Journal*, vol. 5, 2017, *www.isaca.org/Journal/archives/Pages/default.aspx*
2 Actually, there are three if you include downtime caused by cyberattacks, yet another broad hint for future consideration.
3 *Op cit,* Ross. In my research for the previous article, I found that Nintendo uses this term for some of its gaming products. Obviously, I do not mean the term that way and will no longer make excuses for using it. However, I now find that IBM uses the same term for some of its AIX systems, and it is also used with regard to some Unix-based operating systems. I wish there were a more appropriate term for a single console that provides visibility into numerous unintegrated platforms and networks, but I cannot think of one. Suggestions are welcome, but until someone comes up with something better, I am sticking with "virtual console."
4 I have been referring to multi-modal *environments* and here use the word *architectures*. They are not the same thing, with the former implying operations and the latter design. To the extent that organizations operate by design—and there are many exceptions—I think the terms can be used interchangeably.
5 Ennals, R.; *Executive Guide to Preventing Information Technology Disasters*, Springer Verlag, London, 1995. Gouge, I.; *Shaping the IT Organization—The Impact of Outsourcing and the New Business Model*, Springer Verlag, London, 2003. The literature on responsibility and accountability with regard to IT outsourcing is voluminous. These are two enlightening examples.
6 *Ibid.*, p. 97
7 Very American, I know, but the image is a good one.