The Residual Data Center

It is no great secret that organizations are moving more and more applications into the cloud. In fact, a recent research study states that by 2021, 53 percent "of all IT and data processing requirements will be in the cloud, a significant increase from an average of 41 percent today."[1] Add to that the number of organizations that are moving their data centers to colocation facilities and it might be reasonable to conclude that in the near future, on-premises data centers will be things of the past.

That conclusion, I believe, will prove incorrect.

The Need for On-Premises Data Centers

There will always be a need for a data center (or centers) within organizations' facilities. (To be fair, there will probably be some enterprises too small to have their own data centers, but they do not have them today either.) I predict that the Residual Data Centers will be tiny compared with those of the past, even those of today, but that the need for security for the sites themselves, the equipment within and the services running on them will be more concentrated, if not any greater, than today. But the resources for providing that security will be reduced, unless we start planning now for tomorrow's Residual Data Centers.

The reason that on-premises data centers will be retained is that there are some applications and services that cannot or should not be run anywhere else. Among the most evident of these are building management systems that operate functions such as heating, ventilation and air conditioning (HVAC); building entry; elevators; video and audio meeting systems; and the devices in the classrooms. It simply makes no sense to manage building environments remotely.[2] Layering telecommunications rates on top of building operations expenses would defy economic logic, as I see it.

There are a number of industries in which an on-premises presence is required. For example, organizations in the financial services industry often rely on market data services. In many cases, these require an on-premises server to connect with their data feeds, and that server needs to reside somewhere on-site (i.e., in a data center). Other industries such as defense contractors have exceptionally high security requirements. If they wish to use cloud-based services, they would have to build a private cloud, which necessitates on-premises equipment. Will hybrid clouds, with some on-premises equipment integrated with public services, ever fully disappear?

Perhaps most critically, there will always be a need for network termination equipment that connects an organization's data lines to a carrier and then onward to one or more cloud-based services. Or, looked at the other way around, there is a need for equipment to deliver services from the cloud to the right user's desktop. This will not change anytime soon.

Protecting the Residual Data Center

Predictions about what information technology will be in the future, even the near future, have proven notoriously ill-advised in the past. And my vision about the continuing need for a residual on-premises data center may not stand up. But as long as people work in office buildings and factories—and I do not see that reality changing for a very long time—there will be a need for a room with

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.

https://bit.ly/2Re9qdl

Steven J. Ross, CISA, AFBCI, 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.

> “(THE) GEAR IN TODAY'S DATA CENTERS IS THE CENTRAL NERVOUS SYSTEM OF THE ORGANIZATION AND WILL STILL BE SO IN THE RESIDUAL DATA CENTER.”

Enjoying this article?

- Read *How Enterprises are Calculating Cloud RIO*. *www.isaca.org/Calculating-Cloud-ROI*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA’s Online Forums. *https://engage.isaca.org/onlineforums*

telecommunications gear to connect them to the outside world.

The corollary is that there will be a continuing cost for maintaining data centers. There will need to be a budget for servers, storage and networking gear, but, as the number of applications and services decline, the cost for IT equipment should diminish accordingly. But what about the room in which these machines will go? One option might be to retain the current, unnecessarily large data center and put less in it. The cost for environmentals (e.g., heating, ventilation, and air conditioning [HVAC]; uninterruptible power systems [UPS]; fire suppression) plus the demand for floor space will militate against holding on to these spaces.

The remaining data center will likely be little more than a closet. Will organizations be willing to make the same investments in mechanical, electrical and plumbing (MEP) gear that they do today? Of course, many enlightened managers will realize that that need still applies. But from what I have seen in closets housing file servers, recognition of the importance of these facilities will be reduced. That is, until something goes wrong.

The Threats to the Residual Data Center

The core of my concern is that the Residual Data Center will be a tempting target for those who would undermine organizations’ security. Imagine the mischief that might be caused by fiddling around with the local files that businesspeople use for decision-making. Even less imagination is needed to foresee the impact of cyberthreats to building management systems. The use of the Internet of Things (IoT) will only magnify the threat of misuse.[3]

Most important will be the threat to those services that connect individual users to the network to the carriers to the world of information, including any applications in the cloud. This gear in today’s data centers is the central nervous system of the organization and will still be so in the Residual Data Center. The danger should be self-evident, but will it be? I fear that the weakness will go unrecognized until it is exploited.

A great deal of attention has been given to the maintenance of security in the cloud. Unfortunately, in many cases, this has not always resulted in security being a critical consideration in the migration to the cloud. The reasons are various, but, in essence, they are the result of the gap between those aware of the risk of cloud computing and those making the decisions about the migration to it.

We in information security (and the other allied professions that make up ISACA’s constituency) are used to being the Cassandras of information technology. It is inherent in what we do that we look into the future and see what might happen. Sometimes, our fears are not immediately accepted by management. Still, we do what we can to prevent them from happening at all. Sadly, it has taken the advent of the era of cyberattacks for there to be general recognition of the harm that can be done and is being done to information systems.

Should I have more confidence in the decision-making that will need to come to pass regarding the Residual Data Center? Yes, the day when all or most applications and services are run off premises is still a long way off, but the speed with which the cloud has been accepted may mean that it may not be that far into the future. So at the risk of raising a false alarm, I am bringing it up now.

Endnotes

[1] Thales and the Ponemon Institute, *Protecting Data in the Cloud: 2019 Thales Cloud Security Study*, USA, 2019, p. 9, *https://www.thalesesecurity.com/2019/cloud-security-research*

[2] I am aware that there are some systems that do support some building functions, especially HVAC, from the cloud. These may be sensible for small stores and offices with a few persons in them. I do not see them being practical for large (especially multitenant) office buildings or factories. Of course, there may be technology just over the horizon that will prove me wrong.

[3] Wlosinski, L. G.; “The IoT as a Growing Threat to Organizations,” *ISACA® Journal*, vol. 4, 2019, *www.isaca.org/archives*