

Someone Else

Running an IT department used to be so simple. The programmers wrote programs; the technicians migrated the programs into production; and the operators ran them. These days, programmers implement systems purchased from a vendor. The techs have their hands full just keeping the infrastructure (or more likely, the infrastructures) up and running. And, more often than not, the programs are running in someone else's data center.

Let me complicate that a bit more. If the operators are running systems at all, they may be running them in someone else's data center, a colocation facility or colo. Many of the applications and much of the infrastructure are, or soon will be, rented from a third party as a service (or, more likely, as-a-service). And each of those services may well have been selected by end-user management with little or no input from IT personnel who specialize in security, reliability, recoverability or interoperability with other systems.

So, organizations are facing problems, if not yet crises, of IT governance, security, risk management and control—the perfecta of ISACA's certifications.¹ If you are a holder of any of these, you ought to be concerned. Frankly, even without those certifications, there is cause for concern. If you are a programmer, technician or operator, you may already be seeing jobs of some colleagues disappear from your organization. Even though someone else is experiencing a talent shortage,² they seem to be on the sell-side rather than the buy-side.³

Restructuring the Way IT Is Done

The concern is not—or at least, not only—vendor management. It is a fundamental restructuring of the way information technology has been done since the dawn of commercial data processing in the 1960s. An organization, whether a corporation or a government agency, was viewed as an organic whole with a consolidated set of information resources. The objective, only imperfectly achieved, but the goal nonetheless, was to have a single base of information that would be apportioned to each business and each authorized individual as needed

to carry out their business. Containing all of IT within an organization gave management the (supposed) ability to secure all of it.

The idea that all of IT could be contained was a chimera. The computers in the data center were powered by someone else (the electric company), communicated via someone else (the telecommunications carriers) and were maintained by someone else (the hardware vendors). Operating and database management systems were certainly not developed in-house. Purchased applications are not new either. But, for the most part, there was a certain degree of comfort knowing that all of these systems were running in an access- and climate-controlled room somewhere in management's own building.

Where Did the Data Center Go?

Today, the data center is everywhere from someone's pocket to the cloud. I am looking at my smartphone and I find applications such as foreign exchange calculation, medical benefits, voicemail and encryption that used to run in data centers. I know that these are applications running in a data center somewhere that I can access through the terminal in my pocket. The point is that both the data center and the terminal used to be in the building to which I had to travel in order to work.

The use of colos is recognition that computer operations and real estate are separable. The organization had a data center that was built around many basic controls: who could enter, how fires would be prevented, how power failures would be managed, how recovery would be carried out if there were a disaster. Now, those controls are someone else's problem.

And, when information and the systems that support it disappear into the cloud, management's ability to exercise control over them becomes even more tenuous. Depending on what services for which a particular business function contracts, someone else—the cloud vendor—may be

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/2X6cpVv>

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.

Enjoying this article?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. <https://engage.isaca.org/onlineforums>



producing the total environment: the application, the infrastructure and the data center. The cloud is, after all, just a group of interlocked data centers. With every business unit and, for that matter, every individual, free to acquire its own whatever-as-a-service, management's ability to control the use of information within an organization just vanishes.

Objections to the Argument

I am not deaf to the arguments that can be made to what I am saying here. "That may be someone else's problem, but it is not mine. My organization still has plenty of applications running in our data center." That may be the case today, but both market trends and vendor decisions are moving away from on-premises systems.⁴ In many cases, cloud-based applications are already running alongside older on-premises versions in a hybrid configuration.⁵ If the movement out of the data center is not occurring in your organization today, it will be tomorrow.

“ THE USE OF COLOS IS RECOGNITION THAT COMPUTER OPERATIONS AND REAL ESTATE ARE SEPARABLE. ”

Another objection is that the trends that I am describing are actually positive for security and control. Maybe the colo or the cloud service provider does a better job at a lower cost than your organization could ever do, but there is still the matter that the best way to make something disappear is to declare it to be someone else's problem.⁶ There is also the opposite point of view, that "Security will continue to be an issue with cloud technology, especially now with the introduction of the [EU] General Data Protection Regulation (GDPR). Given the advantages of cloud computing, many organizations will likely rush into it without serious consideration of the security implications."⁷

The issue as I see it is not whether the movement away from in-house development and operation of

information systems is better or worse for information security. It is different. Personally, I think the positives outweigh the problems, but those problems will not go away without addressing them head-on. The challenge, I propose, is that many of the verities that could be relied upon for decades are no longer operative. You cannot build security into applications or infrastructure if you do not build applications or infrastructure. The walls of the data center are no barrier if you have no data center and, thus, no walls. You can assure yourself that someone else's security professionals are taking care of things. But, in the end, your security is not someone else's problem; it is yours.

Endnotes

- 1 ISACA®, ISACA Certification, Certified Information Systems Auditor® (CISA®), Certified in Risk and Information Systems Control™ (CRISC™), Certified Information Security Manager® (CISM®), and Certified in the Governance of Enterprise IT® (CGEIT®), www.isaca.org/certification/Pages/default.aspx
- 2 Manpower Group, "Solving the Talent Shortage," USA, 2018, [https://go.manpowergroup.com/hubfs/TalentShortage%202018%20\(Global\)%20Assets/PDFs/MG_TalentShortage2018_lo%206_25_18_FINAL.pdf](https://go.manpowergroup.com/hubfs/TalentShortage%202018%20(Global)%20Assets/PDFs/MG_TalentShortage2018_lo%206_25_18_FINAL.pdf)
- 3 Hickey, A.; "Shortage in Cloud Talent as Cloud Job Seekers Lag Employer Demand," *CIO Dive*, 6 December 2018, <https://www.ciodive.com/news/shortage-in-cloud-talent-as-cloud-job-seekers-lag-employer-demand/543674/>
- 4 Samuels, M.; "Cloud Computing: Five Key Business Trends to Look Out For," *ZDNet*, 14 January 2019, <https://www.zdnet.com/article/cloud-computing-five-key-business-trends-to-look-out-for/>
- 5 Ashok, A.; "Four Trends in Cloud Computing CIOs Should Prepare for in 2019," *Forbes*, 5 July 2018, <https://www.forbes.com/sites/forbestechcouncil/2018/07/05/four-trends-in-cloud-computing-cios-should-prepare-for-in-2019/#35656e394dc2>
- 6 For in-depth research on this phenomenon, I recommend: Adams, D.; *Life, the Universe and Everything*, Del Rey, USA, 1982, chapter 3.
- 7 *Op cit* Ashok