

CISOs in the Cloud

Here is an unoriginal observation: The Cloud changes everything. Oh, wait, that was the Internet. Whatever. It seems that if it is novel, it changes everything. So the Cloud makes most of us information security professionals unnecessary. After all, those fortunate few employed by the cloud service providers (CSPs) will take care of everything for us.

If anyone detects a bit of snark in the paragraph above, the reason is I intended to be a little snarky.

While the cloud does certainly alter the rules of engagement for protecting an organization's information resources, it just as certainly does not eliminate the need for an information security function. I would like to make the case that the movement of those resources into the cloud makes the chief information security officer (CISO) and her or his minions even more important.

What CISOs Do

It is a bit difficult to speak authoritatively about how the CISO's position is changing since, in my travels, I have not encountered two CISOs who see the job exactly the same way. There is too much variation depending on industry, organizational scale, technology and, to an extent not usually recognized, the personality and political skill of the individual CISO. That said, there are some commonalities that I believe most CISOs would recognize.

Most CISOs are responsible for issuing and enforcing information security policy and standards. They conduct risk assessments and, on that basis, set short- and long-term strategies. They keep their antennae raised to detect emerging threats and communicate them both to senior management and throughout their organizations.

Most, if not all, CISOs also have tactical responsibilities.¹ Monitoring information system usage for attacks and misuse is, as I see it, the most common component of all CISOs' roles. And then, if and when there is a breach, they manage the response to security incidents.

I said that it is hard to typify what CISOs do; it is even more difficult to state definitively how organizations are currently using cloud services. Some do little more than acquire a few Software as a Service (SaaS) products. Others use the cloud only minimally for archival storage or data backups. Some are in a transitional period, having lifted and shifted their data centers to those of CSPs. For them, the need for security of their information resources is little changed except at the physical layer. Finally, there are those who have re-engineered the way they manage and use information.

What CSPs Do for Security

The common element in all these uses of the cloud is that they relate to services, which are achieved, in part, by transferring facilities and the equipment involved from a customer's site to a CSP's. So, if movement to the cloud (supposedly) reduces the role of a customer's information security function, what security does the CSP provide?



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?

- Read *Continuous Oversight in the Cloud*. www.isaca.org/continuous-oversight
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. <https://engage.isaca.org/online-forums>



Let a few of the major vendors explain:²

- "Security and Compliance is a shared responsibility between AWS and the customer."³
- "Google is committed to doing its part in keeping your projects secure, but security is a shared responsibility."⁴
- "As you consider and evaluate public cloud services, it's critical to understand the shared responsibility model and which security tasks are handled by the cloud provider and which tasks are handled by you."⁵

So then, what exactly is the CSP's share of the responsibility? The answer differs a little from vendor to vendor, but not much.

Amazon Web Services (AWS) says that it is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking and facilities that run AWS Cloud services. (An accompanying diagram on its web page places hardware and its global infrastructure, plus software for compute, storage, database and networking, in Amazon's zone of responsibility.)⁶

Google states its case differently. Its web page on shared security commits the vendor to security over data center physical security, server and software stack security, trusted server boot, and data access and disposal.

Microsoft Azure takes full responsibility for physical hosts, the network and the facilities. It agrees to some responsibility for identity and directory infrastructure, applications, network controls and operating system(s), based on "service types." The exact extent of Microsoft Azure's responsibility is not spelled out in its literature, although I am quite sure that it is in their contracts.

Reduced to the essentials, these three companies, rather dominant in the marketplace,⁷ seem to me to be saying to their customers, "We will take care of

what is ours. You take care of what is yours." That is not really unfair, but it certainly does raise the stakes for those CISOs whose organizations are migrating to the cloud.

What CISOs Must Do

CISOs are now called upon to keep their own applications and information secure and to ensure that someone else⁸ is doing the same with their applications and infrastructure. I think it is fair to say that most CSPs offer little transparency into the details of their security measures. This is justifiable since they do not want to offer a road map to cyberattackers and, so far, their defenses seem to be generally effective. While there is no shortage of Cassandras who tell of the potential for attacks on CSPs,⁹ the only significant case I know of was the incident involving the US's Capital One Bank at AWS, and that case involved insider information.¹⁰

“IF EVER THERE WAS A TIME THAT INFORMATION SECURITY HAS TO BE A FORETHOUGHT RATHER THAN TAKEN UP AFTER KEY DECISIONS ARE MADE, THIS IS IT.”

In addition to everything that CISOs had to do when all of their organizations' information resources were on premises (and, as I have written before, there will always be a residual data center¹¹), they must now take on additional duties. In particular, they must occupy key roles in vendor selection and management. If ever there was a time that information security has to be a forethought rather than taken up after key decisions are made, this is it. Selecting cloud vendors is less like a purchase and more like a marriage. The vendors make it easy to enter into a relationship and oh, so hard to get out. The degree of commitment dictates early and

ongoing attention to the security of applications, information and infrastructure, both in the cloud and in the building.

Ah, to be a CISO now that the cloud is here.

Endnotes

- 1 Or do I have it backwards? The CISOs I am familiar with are in quite strategic roles, but perhaps there are more who are focused more tactically.
- 2 Amazon, Google and Microsoft are three of the largest cloud vendors and are listed in alphabetical order. There is no way to represent the position of *all* CSPs, but I have not encountered any that do not adhere to a shared security model.
- 3 Amazon Web Services, Shared Responsibility Model, <https://aws.amazon.com/compliance/shared-responsibility-model/>
- 4 Google, Google Security Overview, <https://cloud.google.com/security/overview>
- 5 Microsoft Azure, Shared Responsibility in the Cloud, <https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>
- 6 *Op cit* Amazon Web Services
- 7 Dignan, L.; "Top Cloud Providers 2019: AWS, Microsoft Azure, Google Cloud; IBM Makes Hybrid Move; Salesforce Dominates SaaS," ZDNet, 15 August 2019, <https://www.zdnet.com/article/top-cloud-providers-2019-aws-microsoft-azure-google-cloud-ibm-makes-hybrid-move-salesforce-dominates-saas>
- 8 Ross, S.; "Someone Else," *ISACA® Journal*, vol. 4, 2019, <https://www.isaca.org/archives>
- 9 The most egregious I have read is: *Dark Reading* Staff, "Cloud Customers Faced 681M Cyberattacks in 2018," *InformationWeek Dark Reading*, 24 January 2019, <https://www.darkreading.com/attacks-breaches/cloud-customers-faced-681m-cyberattacks-in-2018/d/d-id/1333721>, quoting a security consultant. Sure they did and why stop at 681 million? But how many of them were *successful* cyberattacks? This statistic is unmentioned.
- 10 Fitter, E.; K. Weise; "Capital One Data Breach Compromises Data of Over 100 Million," *The New York Times*, 29 July 2019, <https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html>
- 11 Ross, S.; "The Residual Data Center," *ISACA Journal*, vol. 1, 2020, <https://www.isaca.org/archives>

