Deloitte.

Who is responsible for cloud security? It might not be who you think.

Government agencies and cloud providers share the responsibility of making cloud more secure

Contributors: Timothy Li, Anil Ramcharan, and Mason Evans

MAKING AN IMPACT THAT MATTERS since 1845

Like many of you, I rely on my internet service for everyday activities at home. I recently had an issue with my internet that illustrates the topic I'm going to cover today. I once fancied myself a network engineer and so I began to troubleshoot the error. I had so many questions. Was it my router? Was it the wireless access point? Was it the fiber interconnect? Was it inside/outside the house? Who do I call first? I truly failed to understand the ecosystem of providers that delivered my precious internet service. Cloud services are very similar in this regard; a utility model that is easy to set up and use, but often very difficult to understand who is responsible when things go wrong.

Cloud can be more secure than most on-premises operations, especially when they leverage the significant resources and tools of large service providers. However, an accurate view of risk is only possible when security is implemented completely, and the varied nature of cloud services can make it difficult to understand who is responsible for each aspect of security. This situation can be even more acute for government, where the assurances of FedRAMP authorizations can lead agencies to believe that cloud service providers are fully responsible for securing the cloud – which is just not true. Without careful analysis, documentation, and stakeholder communication, the complex environment of cloud can create less certainty about roles, increase complexity, and create security gaps that can lead to serious incidents.

With more government data being hosted in the cloud – an estimated 83% of all enterprise workloads are now in the cloud – taking the time to achieve clarity in security roles has never been more important.[1]

There are several key considerations when assessing the myriad of responsibilities and stakeholders in, and around, cloud service offerings

1 **Cloud Service Providers (CSPs) each have different, and competitive, operating models – don't assume they all address cybersecurity requirements in the same way**

Not all CSPs are created the same way. Each CSP operates with different goals: getting a solution to market faster, keeping up with competition, becoming a leader in a niche market, to name a few. In addition, each CSP meets and applies security in a different way, so you can't assume security will be uniform across CSPs, even for a similar service.

There is a myriad of authorizations, such as FedRAMP and StateRAMP (among others), that seek to standardize a level of security. You should be aware of how a CSP meets those requirements and determine if their approach aligns to your security goals. Cloud service security is nuanced. Avoid making assumptions about the CSPs responsibilities. You should engage with the CSPs to really get into the fine print on what they are responsible for delivering as agreed in the terms of service, review their system security plan, understand the CSP's cybersecurity operations, especially how they are meeting authorization requirements, and clearly define and be comfortable with the federation of responsibilities.

It is also important to review what cloud authorizations apply to your situation so that you can define the requirements for those authorizations and where the CSP's responsibilities end and yours begins. A common mistake is to assume that because a cloud service offering is authorized, the responsibility for cybersecurity has been met. Organizations must extend business, regulatory, and operational security policy into cloud services. For example, State government agencies deliver a myriad of services (e.g., Medicaid benefits, health insurance exchanges, and unemployment programs) to their citizens which often bring stringent compliance and data protection dependencies from these cloud services. This is especially true as you use multiple CSPs or multiple offerings or models withi a CSP, both of which are increasingly common scenarios.

As you configure, customize, and use more cloud services, you, not the CSP, are responsible for securing the services, interactions between services, and even the CSP environment itself (e.g., securing access to the CSP console). Security must be evaluated holistically from a risk perspective to include high availability and disaster recovery considerations.

Given the questions outlined in this section. We recommend the following actions to help gain a more detailed understanding of the services and responsibilities:

- Review CSP-provided system security plans (SSPs) / templates and other attestation documents to gather a more comprehensive understanding of how security controls were addressed. This information is considered confidential and will likely require a non-disclosure agreement (NDA) to gain access.
- Establish a dialog with the CSP on its view of customer responsibilities for the services in scope for your engagement. Understand how those responsibilities change by service offering and impact your operational objectives for the service.
- Develop a portfolio of services that must be considered as part of your service design process and policy-driven constraints on the use of those services

2 Cloud engagements that scale to multiple CSPs must clearly define the handoffs and interfaces related to cybersecurity activities and closely manage the crossover in responsibilities

Government agencies are increasingly moving to using multiple CSPs, especially in integrating SaaS offerings, adding complexity to the operating level relationships of mission applications and their protection and defense. Service agreements must clearly delineate the responsibilities, hand-offs, and interfaces as well as the integration of a continuous cyber defense model across difference providers. Once the responsibilities of all parties have been codified, they must be executed and enforced. These hand-offs in responsibility present moments of elevated risk and must be scrutinized, exercised, and managed accordingly. This is especially true in incident response, where each function in the event maintains cohesion to preserve critical elements, such as chain-of-custody.

In the government and public sector marketplace, very rarely is one agency or component the sole participant in a cybersecurity event. Ensure that service agreements include flexibility and provisions for executive actions directed by outside authorities (e.g., DHS US-CERT, USCYBERCOM). Incident response is a team effort, particularly for Federal agencies. CSPs are a key part of that team. For example, as cloud-native applications and services evolve, multi-cloud microservice architectures and the associated cybersecurity model can place significant demands on response teams during the post-preparation phases of the incident response life cycle. Do service agreements have the facility to compel dedicated CSP resources to the incident response teams? Are those resources fit for the type of activities necessary to recovery from a priority incident? Can multiple CSPs work together in the best interest of a client organization to protect and defend its data? These issues require careful consideration early in the cloud adoption phases to remove barriers and friction to an effective cyber defense and response.

In trying to prevent incidents, you will need to validate and enforce the responsibility of the CSPs to meet system and data access requirements across the board. For instance, if you have a requirement for only US-based personnel be allowed access to systems, is the CSP aware of their responsibility to meet this requirement in all aspects of its operations including items like physical security, development, operations, and maintenance, etc., or are they outsourcing certain aspects? You must consider how you will enforce these responsibilities and make sure that during execution, you do not have rogue activity that exploits those responsibilities.

In addition to physical access, access and security of data is an important aspect of all cloud engagements, but especially multi-CSP engagements. You need to be aware of what data is flowing between CSPs and how it is protected. The responsibility for making sure these are configured correctly needs to be clearly defined. For SaaS platforms, the CSP is responsible for meeting data protection requirements, while for non-SaaS platforms, it will likely fall on you to validate you are using the correct configurations and security controls, while maintaining functionality across CSPs. For instance, if you encrypt data at rest using a key management service provided by the CSP, will you be able to unencrypt that data for use in another CSP? As with all aspects of using multiple CSPs, you must make sure all parties involved are aware of what their responsibilities are and where party's responsibilities start and stop.

For multi-cloud environments with complex technical interconnections, we recommend the following actions:

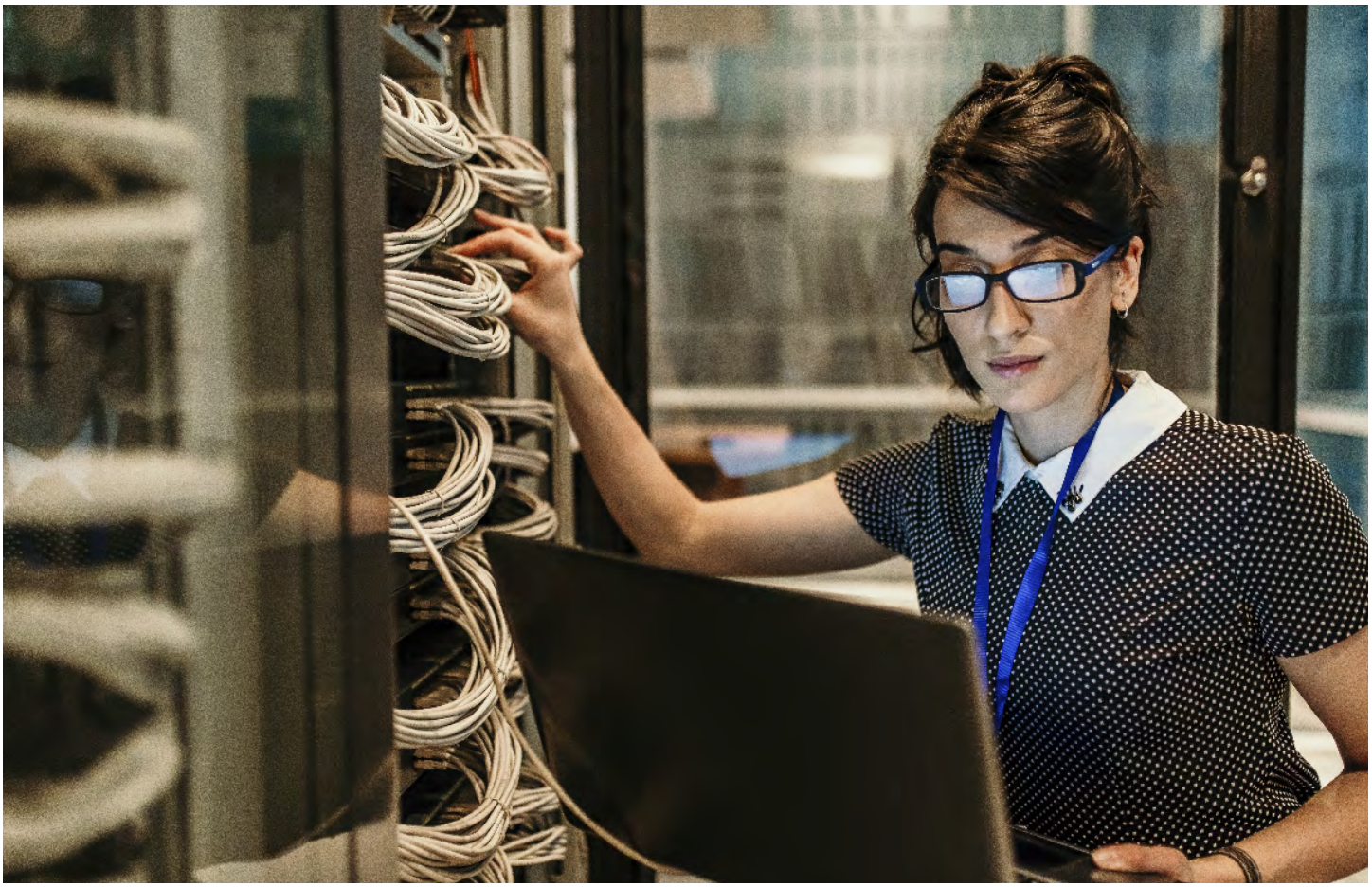
- Develop a risk-based map of incident use-cases to elements of your service catalog or architecture to identify touchpoints/ hand-offs
- Review service- and operating-level agreements for triggers, thresholds, inputs, outputs, and exclusions
- Facilitate table-top and/or operational exercises to prepare and understand the pace and interactions necessary for an actual event.

3 Cloud services represent a complex ecosystem of interconnected suppliers whose relationships, nuances, and dependencies must be understood

While cloud services may initially seem straight forward – you can use what you need without having to worry about the underlying systems and configurations to make the service work. The delivery of these services is "anything but simple" behind the scenes, and often is a closely coordinated effort of the CSP and other related vendors/subcontractors/suppliers. This complicates the cyber threat landscape and begs the question. Does each organization and supplier understand their responsibilities, and are you comfortable with, the different suppliers involved in the ecosystem to make the cloud service work? Often, the terms are accepted without discussion. If there is a question, the CSP may be hesitant to provide details citing the confidential nature of the relationships.

The ecosystem may also vary widely on the services consumed. The spectrum of considerations ranges from fully managed services, which have complex interrelationships, to simple storage services that may be delivered more organically. Another critical ecosystem component is the open-source nature of software used in the delivery of cloud services. It is important to understand if the CSP addressed potential vulnerabilities and understands threats in the open-source software (OSS) supply chain beyond the fact that the software is fit-for-purpose.

- Review open-source collaborations, contributions, and provenance for potential risk
- Assess CSP open-source analysis procedures to determine adequate risk and vulnerability mitigation steps
- Understand any third-party relationships required to deliver fully managed services.



Cloud security is hard work, but the benefits are worth it

Clarifying the wide variety of roles and responsibilities of securing the cloud can be hard work, but it can certainly be worthwhile when it is implemented fully. Data shows that, overall, cloud is a more secure option for most organizations. Despite the increasing use of cloud, cloud assets were involved in only 24% of breaches last year compared with 70% for on-premises.[2] Government organizations need to work closely with cloud service providers to define roles and responsibilities of security the cloud, providing the government confidence that not only will cloud works, but that it is secure. This can be a daunting prospect for any organization, given the questions raised. Where do you start? Which services are the most likely concern? What strategies and leading practices can you employ to get answers and inform key decisions?

Cloud can enable verifiable security when responsibilities are clearly defined, and a realistic adoption strategy is implemented in consideration of the risks and capabilities that are unique to the government organization. Please stay connected with our team directly and via social media as we probe these questions further and seek to illuminate and explore the decisions surrounding cloud service responsibilities.

Endnotes:

1. https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/?sh=74180bac6261
2. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Deloitte.