Dividing Responsibility Among Stakeholders

Key Considerations

- ***Responsibility is divided differently for consumer and enterprise customers.*** The division of responsibility for cloud surety between cloud providers and their customers differs across customers. With major enterprise customers, cloud providers often negotiate contracts that detail who is responsible for issues such as identity and access management, change management, and recovery in the event of cloud incidents. For most consumer cloud services, however, responsibility for these key surety issues is allocated by the cloud provider and detailed in its terms of service.
- ***Unclear and divergent perspectives.*** Industry and government perspectives concerning who is responsible for what vis-à-vis cloud surety are unclear and sometimes divergent. This is especially true with respect to the role of government in supporting cloud surety (for example, by providing assistance in the case of attacks by nation-state actors). However, in practice, stakeholders are trying to better understand where the government may step in, as cloud providers are becoming increasingly aware that cloud surety requires collaboration and coordination with their customers, governments, and other relevant entities (such as insurers and managed security service providers).[1]
- ***Difficulties addressing cross-border issues.*** The development of a coherent model to address cross-national challenges raised by cloud adoption may be constrained by jurisdictional limitations on national or regional responses (such as regulators' mandates, geographies, and national vs. multinational authorities), bureaucratic fragmentation, and divergence in different governments' political interests.
- ***Limited understanding of cloud technology and operations.*** National governments' and multinational institutions' regulatory approaches are limited by their ability to understand and audit the cloud industry's services and operations. Efforts to develop uniform solutions are also hindered by variations in the characteristics of cloud services, sectors, functions, and threat vectors (for example, organized crime, state attacks),[2] as well as the different service models offered by the various cloud providers. Moreover, the rapid evolution of the technology and cloud providers' business practices, as well as considerable variation in their contractual arrangements with their customers, further complicate efforts by their customers (including governments) to understand, and adjust, their own third-party dependencies.

Background

Providing cloud services involves many stakeholders—including but not limited to cloud providers, governments, and enterprise customers—working together. As a result, these parties must also cooperate to ensure the surety (security, robustness, and resilience) of these services. However, as cloud services, business models, and contracting have evolved, it has become increasingly difficult to identify who is responsible for what. This section provides a series of templates that can serve as a starting point for these stakeholders, as well as others, including managed security service providers[3] and insurers, to begin identifying and dividing these responsibilities.

Clearly dividing responsibilities has obvious benefits for cloud providers and their enterprise customers, who can avoid confusion and disputes with one another in the event of a cloud incident. It can particularly benefit smaller customers of cloud services, who may lack the knowledge and power to shape the allocation of responsibility when negotiating contracts with their cloud providers. Larger enterprise customers may have chief technology officers and legal teams to help steer contract negotiations, but they may nevertheless face power asymmetries with cloud providers that stem from unfamiliarity with cloud computing technology or the broader cloud services landscape, which these templates could help offset.

This effort comes from our analysis of how major cloud providers currently divide such responsibilities.[4] This reveals considerable variation on three issues:

1. ***Which controls are identified?*** Of the models reviewed, most account only for cybersecurity controls while very few account for robustness (for example, physical infrastructure hardiness) and resiliency controls (such as disaster recovery).
2. ***How granular is the division of responsibility?*** Some cloud providers give very high-level indications of the distribution of responsibility (for example, the cloud provider is solely responsible for the security of the virtualization layer), and others provided more granular information (such as for SaaS, providers and customers share the responsibility for incident and operations management at both the level of the software packages and the operating system).
3. ***Does the division of responsibility change depend on service type?*** Although the majority of cloud providers offer models that are disaggregated by service type (such as IaaS, PaaS, SaaS), several produced only a generic model.

Moreover, providers' published models for dividing responsibility do not identify a clear role for governments (for example, in attribution, response to state or state-sponsored attacks, whole-of-system cyber risk management, and so on). However, in practice, cloud providers and their customers increasingly recognize that there is a need to clearly define the role of governments in supporting cloud surety, beyond cases wherein cloud incidents threaten government services or critical infrastructure.

Templates

The current state of uncertainty and tension has created a patchwork of individual efforts and unclear expectations of stakeholder roles and responsibilities, especially with respect to issues where government participation is welcomed or necessary. Such complexities point to the necessity of developing new approaches that focus on building and sustaining trust among stakeholders.[5] With this in mind, we have developed an approach to outlining the division of roles and responsibilities among all three stakeholders (governments, cloud providers, and their customers), illustrated in the following three templates.

[Insert Templates Here]

Notes

[1] Office of Management and Budget, “Cloud Smart,” Office of Management and Budget, June 24, 2019, https://www.fedscoop.com/final-cloud-smart-policy/

[2] Phil Goldstein, “How the Cloud Can Help States Process Unemployment Claims Faster,” *StateTech*, May 8, 2020, https://statetechmagazine.com/article/2020/05/how-cloud-can-help-states-process-unemployment-claims-faster