North American Broadcasters Association (NABA)

Initial Cyber Security Recommendations for Public Cloud Services

The use of cloud is now ubiquitous in the broadcasting/media industries. Cloud services offer the broadcaster the ability to flexibly spin up and down additional storage and compute capacity whenever required.

As cloud clients, broadcasters should understand the controls in place to protect broadcasters'data. It is important to assess both broadcasters' internal level of assurance, and the level of assurance offered by the cloud service providers.

The National Institutes of Standards and Technology (NIST) Publication 800-145 provides definitions and a conceptual framework for Cloud Computing. This Publication has identified Cloud Service and Cloud Deployment Models that are now used ubiquitously throughout the industry. Service Models include: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Deployment models include: Private Cloud, Community Cloud, Public Cloud and Hybrid Cloud.
A clear distinction must be made between service models (PaaS, IaaS and SaaS) and deployment models (Private, Public and Hybrid).

Responsibilities vary depending on the service model chosen (See Figure 1). Most cloud contracts make the customer ultimately responsible for security, data protection and compliance with local laws. The cloud service provider's liability is restricted; apart from infringement claims relating to intellectual property. The maximum service provider liability is usually limited to a maximum of the value of the fees over the past twelve months.

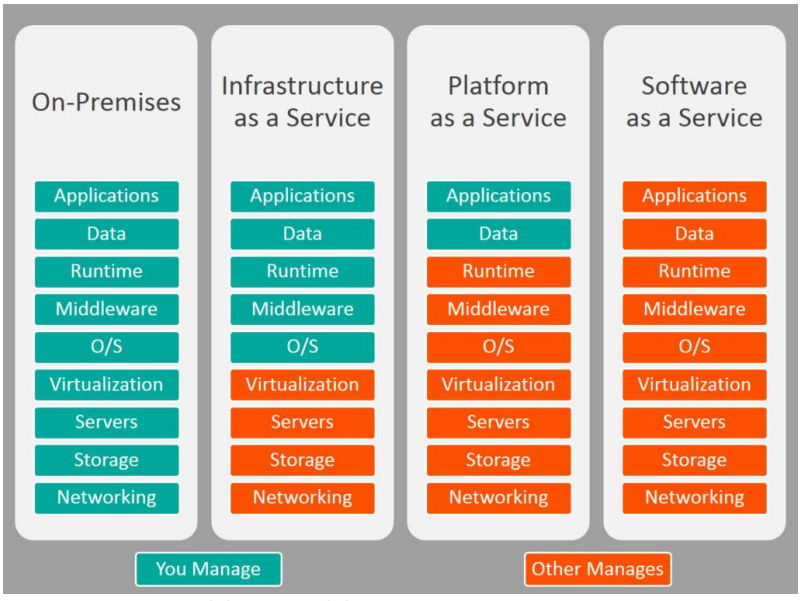

Figure 1- Service models responsibilities

The type of cloud services considered in this document are third-party public cloud services ("Cloud Service Providers, or "CSP"), which include companies such as Amazon, Google, Microsoft, etc., and only for IaaS deployment models.

When considering the use of a cloud service provider, broadcasters should first review their business requirements and engage the services of the internal enterprise CISO or Information Security team in order to assess the risks associated, and establish an indication of best practices and validate the security posture of their cloud offerings in order to meet security, confidentiality, and compliance requirements. An acceptable level of maturity must be accepted by the organization.

It is also critical when engaging with your IaaS provider to understand the "shared responsibility" model for security in those cloud computing environments. In reality, most cloud service providers can deploy multiple cloud service models. It is the responsibility of the broadcaster to understandwhich security controls are provided by the cloud service provider and which are their own responsibility. Often the security facilities provided by the cloud service provider are not strictly analogous to on-premise controls and require additional training and experience to understand their functioning completely. In short, the "security *of* the cloud" is typically managed by the cloud service provider and "security *in* the cloud" is manged by the broadcasters..

The sensitivity level of the information to be stored in the cloud should be assessed according to the approved classification policy prior to engaging. A privacy impact assessment should be undertaken in the case of confidential or restricted information and specifically in case of personally identifiable information (PII).

In addition, availability of the service provider tools such as Business Continuity and Disaster Recovery plans of the cloud service provider should be thoroughly assessed.

There already exists a number of published recommendations, certifications, audit material, etc. associated with cyber security and cloud services. The following are some representative examples, but not a definitive list.

NIST Standards

- **NIST 800-145: The NIST Definition of Cloud Computing.**

Vendor and industry Standards

- American Institute of Certified Public Accountants (AICPA) – System and Organizational Controls (SOC) for Service Organizations, including SOC 1, SOC 2 and SOC 3
- International Organization for Standardization (ISO) 27001, ISO 27017, ISO 27018, ISO 17788, ISO 17789, ISO 9001, etc.
- The Security Trust Assurance and Risk (STAR) Program

Cloud Vendor and Customer Standards

- Cloud Security Alliance (CSA) Cloud Control Matrix
- Center for Internet Security (CIS) Benchmarks for AWS, GCP, Microsoft Azure, etc.

Broadcasting Unions' Recommendations

- European Broadcasting Union (EBU) Recommendation R146: "Cloud Security, including Procurement, Architecture and Cloud Service Provider Assessment"

July 2, 2019