North American Broadcasters Association (NABA)

Initial Cyber Security Recommendations for Software as a Service (SaaS)

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 by the cloud service provider 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.

The type of cloud service considered in this document is third-party Software as a Service. These vendors are now becoming prevalent in industry and many previously on-premise client software applications are moving to a SaaS model. SaaS provides the convenience of relying on the third party to maintain the application, update new features and run the underlying infrastructure to deploy the application. Many times, the SaaS provider employs a public cloud provider as its infrastructure. In addition, most SaaS services are available everywhere a user can get an Internet connection, so flexibility and collaboration are enhanced.

On the other hand, SaaS presents challenges to the enterprise, such as the following examples: :

- SaaS vendors may be smaller companies without dedicated security teams;
- With SaaS, Internet connectivity is required, so "air-gapping" (or physically separating) networks is no longer an effective security control;
- User access control may be more complicated if user accounts are managed by the SaaS service provider;
- Account databases may not be sufficiently secured with strong crypto-libraries and appropriate algorithms/key management protocols;
- Ubiquitous access places a burden on the broadcasters' security team to conduct threat modeling in order to ensure that the level of access does not allow for insider or external threats;

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 SaaS provider to understand the "shared responsibility" model for security in those cloud computing environments. With a SaaS service, the SaaS vendor is responsible for security up to and including the application layer. Broadcasters' responsibility with SaaS vendors is focussed in doing due diligence that the SaaS service provider have secured their infrastructure and applications appropriately. Currently, the Trusted Partner Network (TPN), a CDSA and MPAA joint project, conducts security reviews for a number of SaaS vendors in the media/broadcasting industries, using a fairly rigourous standard.

Initial Cybersecurity Recommendations in SaaS environments:

1. Conduct a review of the SaaS provider's overall security organization and posture, or reference one conducted by a responsible third-party;
2. Identify broadcasters' enterprise admininistrators and determine how much control over security settings a broadcaster can assert through the administrators' consoles for the SaaS application;
3. Enable SSO integration and multi-factor authentication, wherever feasible;
4. If account management is conducted by the SaaS vendor, determine how user access reviews can be conducted and ensure that the credential database is secured appropriately. Advise users not to use their enterprise credentials with the SaaS vendor, unless it is with SSO;
5. Determine how Role-Based-Access control is handled;
6. Determine the level of auditing provided by the SaaS application and whether access is provided to the broadcaster
7. Determine how security breaches are handled by the SaaS vendor, including notification delay, communications, updates and post-mortems;
8. The use of a CASB, a Cloud Access Security Broker, is recommended. This tool can be placed inline at broadcasters enterprise perimeter and/or connected via API to cloud SaaS vendors;
9. Determine the broadcasters relevant corporate policy with regard to the access of the SaaS platform when not on-premise and when not using an authorized company device. Use of SaaS usually requires an analysis of your company's mobile and BYOD policies and management, such as MDM or MAM;

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

In addition, availability of the service provider services 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 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