Cloud Security Due Diligence

By Chris Wolski – ISSA member, Delaware Valley (Philadelphia, PA) Chapter

This article discusses the importance of understanding and level of effort required for mitigating risks that third-party cloud services (SaaS, IaaS, and PaaS) represent to an organization. Depending on the service, it may not be possible to conduct a thorough direct assessment of the services, which is necessary to ensure securing the organization's data.

Abstract

This article discusses the importance of understanding and level of effort required for mitigating risks that third-party cloud services (software-as-a-service, infrastructure-as-a-service, and platform-as-a-service) represent to an organization. Depending on the service, it may not be possible to conduct a thorough, direct assessment of the services, which is necessary to ensure securing the organization's data. To overcome this lack of ability, organizations can default to developing a technology survey that asks questions that are considered important security factors. Additionally, organizations may be able to rely on external auditing firms that attest to the provider's level of security and internally developed surveys.

Organizations look to move to the cloud to meet various needs that are met by vendors and developers that offer solutions. However, the security provided by the vendors and developers is not necessarily equal. It is important for organizations to understand how their data is being stored and processed by the cloud solution. To do this, it is recommended that security organizations present a survey to the provider that can be used by the business to determine if a given solution is secure enough to meet its needs. In some cases where the cloud service processes financial transactions, it may be necessary to obtain a third-party attestation that validates the security claims the developer/vendor has in place. It is necessary that the organization do due diligence in protecting the data in the cloud when using cloud-based solutions.

The cloud movement

Since the start of the Amazon Compute Cloud in 2006, the call has been "Go to the cloud." Amazon had become good at providing infrastructure-as-a-service through compute, database, and storage capabilities. Companies and individuals were beginning to realize the benefits of using the various pieces of Amazon's cloud infrastructure. It is easy to get cloud services running, move processes and data to those services, and celebrate the success of reduced costs by not having to maintain their own infrastructure [8].

The move to the cloud, however, is fraught with peril. According to Dark Reading, the top cause for data leakage in 2017 was due to poorly configured security and accidental release of information. They attributed the largest percentage of loss due to poorly configured cloud storage access permissions [5]. Yet, this peril has not dissuaded organizations from proceeding to the cloud.

Following Amazon's footsteps other providers such as Microsoft, Google, IBM, and Alibaba provide similar capabilities. With the increased availability of cloud compute and storage capabilities, developers have rushed to create applications in the cloud environment to resell or supplement their organization's own requirements. Based on NIST's definitions of cloud services in NIST 800-145,[1] there are three categories of cloud services. When an organization licenses software-as-a-service (SaaS), it is getting a cloud-based application that is fully developed, managed, and offered to customers. This differs from platform-as-a-service (PaaS) where the provider takes care of the servers, network, and related infrastructure to provide the customer a place to develop its own applications, store data, and perform computations on that data. When a cloud provider offers infrastructure-as-a-service (IaaS), it provides fundamental elements necessary to per-

1 Peter Mell and Tim Grance, "NIST 800-145 - NIST Definition of Cloud Computing," NIST, September 2011 – https://csrc.nist.gov/publications/detail/sp/800-145/final.

form networking, storage, and computing; the rest is left to the customer.

Different cloud services – Different security responsibilities

There are two areas of concern that require different methods of validating the security of the information stored: 1) software being offered from the cloud (SaaS) and 2) organizations moving IT capabilities to the cloud to meet their own requirements (PaaS and IaaS).

Security challenges related to development or storage of data, such as poor security controls configuration or protection of sensitive credentials, are mistakes that fail to follow openly published and accepted configuration guidance [7]. When organizations take advantage of software-as-a-service (SaaS) solutions without fully ensuring the minimum security recommendations from the cloud hosting provider, the same outcomes could occur.

Organizations that seek to use software-as-a-service must take into account that they don't have control of the cloud services that the application is built upon. Therefore, they will not be able to protect their data that is stored or used by the SaaS solution. The simplicity of purchasing ready-made SaaS solutions makes the cloud attractive as the solutions typically do not require software to be installed on a server or workstation.

In my experience and in discussions with CISOs, to address a need the statement "we need to find a cloud solution" drives business units to make purchases. This may be unbeknownst to the information technology or information security organization tasked with supporting and protecting the business.

Depending on the organization or the type of data, moving data or using cloud services does not relinquish the organization's responsibilities to meet regulatory requirements. If the organization is publicly held with reporting requirements on internal accounting controls, services or applications must be able to withstand external auditing, especially as it relates Sarbanes Oxley [7].

Additional regulatory considerations include Health Insurance Portability and Accountability Act (HIPAA) requirements to protect personal health and information of patients. Non-federal governmental organizations desiring to work with the US Department of Defense must meet requirements to protect controlled, unclassified information that is guided by NIST 800-171.[2]

Plan for security before making the move

NIST Special Publication 800-144 [6] provides guidelines for security and privacy when using public cloud computing. Its first word of caution is to "carefully plan the security and privacy aspects of cloud computing solutions before engaging them." To successfully plan, organizations should:

- Identify and document requirements
- Conduct a risk assessment
- Develop policy governing the use of cloud-based computing
- Implement a procurement process
- Ensure data is encrypted when sending it to the cloud
- Use a desktop/server application if possible instead of a browser to send the data to prevent unintended interception of the data by browser add-ons

2 Ron Ross et al, "NIST 800-171 rev 1 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," NIST, June 2018 – https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final.

- Follow the recommended practices for security provided by the cloud provider

These guidelines are applicable whether the organization is looking to employ SaaS, PaaS, or IaaS.

During the procurement process, a service agreement should be developed and reviewed. The agreement should provide the terms and conditions for access and use of the services as well as subscriber's rights to the data during and after the contract term.

Poor cloud security can lead to unintended consequences

Not only does cloud computing have the potential to expose an organization's data to threats normally found internally, it also adds a new dimension of risks and increased threats by placing it externally. This is typically due to the Internet and the cloud services becoming part of the infrastructure.

The use of PaaS storage services such as Amazon S3 typify a service that organization's use to store data externally either for processing by other cloud services, data backup, or for sharing among organizations. In 2017, open, not-secured Amazon S3 storage buckets were targets of criminals and data hunters alike. According to ThreatPost there were over 22,000 vulnerable storage containers and management services for storage containers inadequately protected [11]. The data included everything from children's voices recorded by a toy to military imagery and data files. Some of these leaks were caused by third parties performing some sort of service for the owner of the data [9].

Another example of how a company that provides services did not follow the recommended practices is Uber. In its case, a leaked password via cloud-based development repository GitHub was the source of the breach. The password was stored insecurely and was used by the attacker to gain access to the company's Amazon AWS resources [10].

Organizations that have adopted a cloud infrastructure may have not followed through with the necessary security settings to protect the data. For example, Accenture left the permissions on their S3 buckets set to be accessible by the public [4].

Unfortunately, many organizations feel a sense of security as the infrastructure belongs to the provider, and therefore it is assumed that security is the responsibility of the provider. This false sense of security has left many data sources and compute resources inadequately protected despite the best efforts of Amazon AWS Educate,[3] Microsoft Virtual Academy,[4] and others to educate their customers to the contrary.

3 Amazon AWS Educate – https://aws.amazon.com/education/awseducate/.

4 Microsoft Virtual Academy Cloud Courses – https://mva.microsoft.com/search/SearchResults.aspx#!q=azure%20security.

Security surveys

To assess the technical and security competency of cloud solutions, organizations should develop a technical survey to get answers that will help determine the security of cloud-based solutions. The survey questions can be lumped into two groups, one for IaaS and PaaS, and the other for SaaS.

IaaS and PaaS solutions differ from SaaS in that those solutions are offered for organizations to build their own environment. In the case of PaaS, it may be a cloud-based co-location site for offsite computing where the organization builds its own servers on cloud-based hardware. For PaaS, it may be the cloud provider's data storage solution, such as Amazon's S3 buckets or Microsoft's Azure Storage [3].

The following questions, with applicable NIST Cybersecurity Framework[5] revision 1.1 subcategories in parentheses and NIST 800-144 sections in brackets, are recommended to be part of the survey for IaaS and PaaS.

Authentication and access control

- Does the service support Security Assertion Markup Language (SAML) or OpenID standards (PR.AC-1) [4.5]?
- Is eXtensible Access Control Markup Language (XACML) used to control access to cloud resources (PR.AC-4) [4.5]?
- Is there an access audit trail (PR.MA-2) [4.3]?

5 NIST Cybersecurity Framework – https://www.nist.gov/cyberframework.

Monitoring

- What auditing requirements have been defined (PR.PT-1) [4.2]?
- What security monitoring requirements have been defined (DE.CM-1,2,3,4,5,6,7,8) [4.3]?
- Do we have access to debug, access, and audit, and if so how are they accessed, stored, and secured (PR.PT-1) [4.3]?

Incident response

- How will my organization be notified in the event of a breach (RS.CO-2,3) [4.9]?
- What is your incident response plan (PR.IP-9, RS.RP-1) [4.9]?
- What can be expected from your service to help remediate the breach (RS.CO-1) [4.9]?

Location

- Where are the data and/or compute resources physically located (ID.AM-3) [4.2]?

Security

- When data is no longer needed, what assurances are provided to prove that the data was destroyed (PR-IP.6) [4.7]?

SaaS security

SaaS applications are typically built upon a developer's use of IaaS and may utilize PaaS as part of its product. Therefore,

questions should be asked in addition to the survey questions for IaaS and PaaS. The following questions are general in nature and are based on NIST's Cybersecurity Framework Revision 1.1. The framework subcategory is annotated in parentheses.

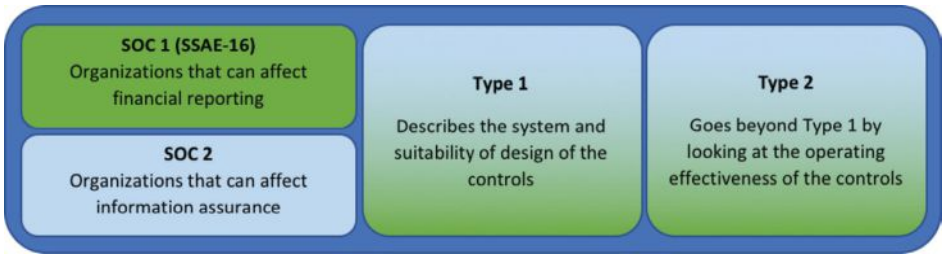

Figure 1 – SOC reports and the different types

Access control

- Does the application support Role-Based Access Control (PR.AC-4)?
- What user privilege levels does the application support (PR.AC-6)?
- What user access restrictions have been defined (PR.AC-4)?
- Does the application support multi-factor authentication (PR.AC-7)?

Environment

- Are the development and production environments separated (PR.DS-7)?
- What procedures are in place for change management (PR.MA-1)?
- What frameworks and programming languages were used to develop the application (ID.AM-2)?
- What client-side dependencies are needed (Flash, Java, Acrobat, etc.) (ID.AM-2)?
- How will database connection strings, encryption keys, and other sensitive components be stored, accessed, and protected from unauthorized access (ID.AM-5)?

Security

- Who maintains the security changes (PR.IP-2)?
- Describe vulnerability management for systems and applications (ID.RA-1)
- How do you ensure that third-party vendors meet or exceed your—and our—security requirements (ID.AM-6)?
- How is information specific to us kept segregated and confidential (ID.AM-3/ID.AM-5)?
- Will our data always be available to us, including after contract termination (PR.DS-4)?
- Will our data be available to us in readable, non-proprietary format (PR.DS-4)?

Get third-party validation of security claims

For services and applications that fall under regulatory compliance requirements, it is best to back up the developer's claims that they are meeting security requirements with a third-party that evaluates the security stature of the provider. This is especially important when organizations must provide proof to a government entity that their information is secured and not subject to tampering.

Major cloud service providers such as Amazon[6] and Microsoft,[7] provide System and Organization Controls (SOC) reports from the Association of International Certified Public Accountants that attest to the physical and system security controls they provide for their SaaS, IaaS, and PaaS services.

The reports you are likely to see are SOC 1 (also known as SSAE-16/18[8]) and SOC 2. For international organizations they may have an ISAE-3402.[9] SOC 1 and 2 reports are broken down into Type 1 and Type 2 reports. Type 1 essentially confirms the organization's description and suitability of the controls to meet the objectives. Type 2 controls go beyond and audit the effectiveness of the organization's security controls. Figure 1 breaks down the two SOC reports and the two possible types.

These documents are significant as they are an attestation by an independent third party on the viability of the security controls in place. When working with a SaaS solution, you should be requesting the SOC document for the cloud provider they are using, as well as the developer's SOC document. For example, Amazon AWS issues a SOC document that attests to the security controls in place for the platform and infrastructure, but not for the SaaS application [2].

SaaS SOC documentation requirements

SaaS applications that depend on cloud services must produce additional SOC documentation that show that the application meets the regulatory requirements the organization is subject to. These documents are in addition to the SOC documents provided by the IaaS and PaaS provider the developers built their applications on. Therefore, in addition to the questionnaire and the IaaS/PaaS SOC documentation, request any documents relating to certification or attestation to the security implemented by the developer for the application. The Association of International Certified Public Accountants developed SOC reports as a method of attestation that is used "to assess and address the risks with an outsourced service" [1].

Smaller and newer developers may not know or have these documents, which according to TrustNet can cost up to $30,000 to be produced [12]. It is important for organizations

6 Amazon SOC Compliance – https://aws.amazon.com/compliance/soc-faqs/.

7 Microsoft Trust Center SOC 1, 2, and 3 Reports – https://www.microsoft.com/en-us/trustcenter/compliance/soc.

8 SSAE-16/18 – Statement on Standards for Attestation Engagements

9 International Standards for Assurance Engagements (ISAE) No. 3402 – http://isae3402.com.

to identify this shortfall early and prior to acquisition of the SaaS product or in the planning stages of the project to ascertain the SaaS solution's ability to complete these documents, with or without the assistance of the organization.

Once you get the answers to your questions, make the decision if the SaaS provider has done enough to meet your organization's security requirements. Think of it as what protections would need to be in place to protect the data if it was in your organization's own on-premise or cloud environment.

Conclusion

When an organization outsources infrastructure, platform services, or software applications to the cloud, the data will be stored and processed outside of its control. It is incumbent that an organization address the risk to the organization's data and compliance requirements.

It is necessary for organizations to exercise due diligence by ensuring the providers of IaaS, PaaS, or SaaS solutions meet basic requirements that will protect the organization's data. This due diligence can be done through a security survey provided to the providers. Additionally, if the data is sensitive and/or falls under a governance requirement, organizations should make the extra effort to request third-party attestation that the providers have met your due-diligence pre-requisites via SOC or equivalent documents.

References

1. AICPA. "System and Organization Controls: SOC Suite of Services," AICPA (2018) – https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html.
2. Amazon. "SOC Compliance - Amazon Web Services (AWS)," AWS (2018) – https://aws.amazon.com/compliance/soc-faqs/.
3. Apprenda. "IaaS, PaaS, SaaS Explained and Compared," Apprenda (2018) – https://apprenda.com/library/paas/iaas-paas-saas-explained-compared/.
4. Cloud Security Alliance. "Security Guidance for Critical Areas of Focus in Cloud Computing v4.0," Cloud Security Alliance (2017, July 26) – https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL-feb27-18.pdf.
5. Higgins, K. "2017 Smashed World's Records for Most Data Breaches, Exposed Information," Dark Reading (2018, February 6) – https://www.darkreading.com/attacks-breaches/2017-smashed-worlds-records-for-most-data-breaches-exposed-information/d/d-id/1330987.
6. Jansen, W. and Grance, T. "Guidelines on Security and Privacy in Public Cloud Computing (SP 800-144)," National Institute of Standards and Technology (2011) – https://csrc.nist.gov/publications/detail/sp/800-144/final.
7. Kuczwara, D. "Knock Your SOX Off: Federal Compliance Rules and the CLoud," TechGenix (2017, January 17) – http://techgenix.com/sox-compliance-cloud/.
8. Miller, R. "How AWS Came to Be," TechCrunch (2016, July 2) – https://techcrunch.com/2016/07/02/andy-jassys-brief-history-of-the-genesis-of-aws/.
9. Mimoso, M. "Vendor Exposes Backup of Chicago Voter Roll on AWS Bucket," ThreatPost (2017, August 18) – https://threatpost.com/vendor-exposes-backup-of-chicago-voter-roll-via-aws-bucket/127538/.
10. Posey, B. "Biggest AWS Security Breaches of 2017," Sumologic (2018, January 24) – https://www.sumologic.com/blog/security/aws-security-breaches-2017/.
11. Seals, T. "22K Open Vulnerable Containers Found Exposed on Net, "ThreatPost (2018, June 18) – https://threatpost.com/22k-open-vulnerable-containers-found-exposed-on-the-net/132898/.
12. TrustNet. "SOC/SSAE 18 Report Cost: SOC Report Cost," TrustNet (2018) – https://www.trustnetinc.com/pricing/soc-ssae18-report-cost/.

About the Author

Chris Wolski, CISO Ascension Global Technology, has over a thirty years of IT security experience. A former US Navy Chief Petty Officer, Chris was responsible for analyzing and reporting on potential threats to the US Navy in his role as a Cyber Threat Technical Analyst. He has an MBA and Bachelor of Science Degree in Cybersecurity. He may be reached at nvycpo69@gmail.com.