State of Cloud Security 2016

CSA Global Enterprise Advisory Board

State of Cloud Security 2016

FOREWARD

The Cloud Security Alliance Global Enterprise Advisory Board, founded in 2016, is a collection of leading experts from large multinational companies representing over 10 unique industries. This board has been constituted to represent the point of view of large IT end users, and to articulate the perspective of the consumers of cloud computing related to the topic of information security. This document is an abbreviated first version of what will be an annual report issued by this board, among other activities designed to raise awareness of cloud computing security and the importance of enterprise end user collaboration.

The quality of IT systems and their inherent security capabilities are related to the demands of the sophisticated consumers from large enterprises and the agenda they set for the industry. We hope your primary takeaway from this report is that the state of cloud security is a work in progress and that it is incumbent upon the cloud user community to collaborate and speak with an amplified voice to ensure that their key security issues are heard and addressed. We welcome your feedback to this report and encourage you to follow our activities.

Web: https://cloudsecurityalliance.org/geab
Email: geab@cloudsecurityalliance.org
Twitter: @csageab

Vinay Patel - Citigroup, Chair

Ricky Arora - British Petroleum

Niall Casey – Johnson & Johnson

Gurdeep Kaur - AIG

Vjay LaRosa - ADP

Pete Nicoletti - Hertz

Jairo Orea – UnitedHealth Group

Michael Panico - Lucas Films

Joe Zacharias - Caterpillar

INTRODUCTION

Cloud computing is an incredible innovation. While at its heart a simple concept, the packaging of compute resources as an on demand service is having a fundamental impact on information technology with far reaching consequences. Cloud is disrupting most industries in a rapid fashion and is becoming the back end for all other forms of computing, such as mobile, Internet of Things and future technologies not yet conceived. As governments, businesses and consumers move to adopt cloud computing en masse, the stakes could not be higher to gain assurance that cloud is a safe, secure, transparent, and trusted platform.

This paper seeks to view the cloud computing industry through the lens of the enterprise information security practitioner. By articulating the state of cloud security from this viewpoint, we can better understand the gaps and solutions we must advocate for and help cloud providers better understand the needs of their consumers.

ADOPTION OF CLOUD

Cloud computing is experiencing robust adoption, as the result of both top-down IT strategic planning and viral adoption from individual users and departments.

Enterprises are overwhelmingly managing hybrid public-private cloud environments and using all major service delivery modes: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). In addition, many other cloud-based services derived from the original S-P-I model have been introduced to the market, such as Data as a Service (DaaS), Security as a service (SecaaS), NaaS (Network as a Service), and Identity as a Service (IDaaS). Enterprises will typically have a wide range of unique cloud services inclusive of all the types defined above. Managing security and compliance of these disparate cloud services is an ongoing challenge to Enterprise customers.

Looked at from the perspective of total IT spend, cloud computing still represents a fairly modest portion of overall spending[1]. This means that the majority of cloud computing adoption has yet to occur and efforts to improve the security of the cloud computing ecosystem now will have a significantly positive impact on the industry. Failure to address security at this stage will potentially “lock in” a default insecure cloud ecosystem.

In instances where cloud computing is not adopted, the consistently cited reasons across several different surveys[2] are:

[1] Network World: Cloud to consume almost half of IT infrastructure sales by 2019 http://www.networkworld.com/article/2944957/cloud-computing/cloud-to-consume-almost-half-of-it-infrastructure-sales-by-2019.html; ComputerWorld: Tech Forecast 2016 http://www.computerworld.com/article/3012628/it-management/forecast-2016-essential-data-points-for-the-tech-year-ahead.html#slide1

[2] eWeek: Cloud Adoption Is Widespread, Despite Security Concerns, http://www.eweek.com/cloud/cloud-adoption-is-widespread-despite-security-concerns.html; RightScale: Cloud Computing Trends: 2016 State of the Cloud Survey http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2016-state-cloud-survey; ComputerWorld: Tech Forecast 2016 http://www.computerworld.com/article/3012628/it-management/forecast-2016-essential-data-points-for-the-tech-year-ahead.html#slide1

- Security
- Compliance
- Lack of expertise and/or resources
- Performance (this may refer to a variety of problems, from ill-suited cloud applications, network bandwidth and other factors)

It should also be noted that in the past 18 months we also see surveys showing that some consumers are adopting cloud computing to actually gain better security capabilities, such as improved monitoring and configuration management.

Cloud computing adoption is solid and increasing. Security and compliance can be adoption barriers. Now is the time to increase the pressure on cloud providers to build security in, not try to bolt it on as an afterthought. The longer it is deployed, the more challenging this task becomes.

ARE CLOUD PROVIDERS SECURE?

While many of the discussions about cloud computing security end up focusing on a handful of the very large name brand cloud providers, the reality is that tens of thousands of unique business cloud services have been identified and classified. As expected, the security of all cloud providers varies widely. The top tier of cloud providers have robust information security programs. At the same time, some nascent cloud providers have no recognizable security program whatsoever. A January 2016 CSA survey[3] showed that 65% of respondents were confident that cloud had equal or greater security than internal IT systems. Some important considerations regarding the state of cloud security:

The level of security program maturity on the part of cloud providers can be impacted by a few factor including the number of years in business, number of customers, industries served and regulatory requirements. The sophistication of customers and their advocacy of security best practices has a positive impact. Many cloud providers will make a security enhancement requested by a customer available to all customers in the effort to maintain a standardized offering.

Integrating and aligning security programs across a cloud provider and an enterprise is a challenge. Historical security best practices and conventional wisdom have focused upon the security of an organization and less so towards ecosystems and supply chains. Thus even a cloud provider with a robust security program and one of its most sophisticated customers may have a suboptimal information security posture in aggregate. There are often communication gaps, such as an inability to share security event information seamlessly between the two parties.

The interdependencies inherent in cloud computing are critical. The ease of development using APIs and rapid deployment in cloud create important security considerations. SaaS vendors often develop applications that don’t fully leverage the security capabilities of underlying IaaS foundations

[3] The Cloud Balancing Act for IT: Between Promise and Peril, https://cloudsecurityalliance.org/download/the-cloud-balancing-act-for-it-between-promise-and-peril/

It is critical to understand that enterprises, particularly those from highly regulated industries, own the accountability for their security posture regardless of who actually manages it. Enterprises want a holistic view of this security posture to see cloud as an extension of their on-premise IT footprint. Enterprises and cloud providers need to agree to look beyond organizational boundaries to hold this common perspective. Greater transparency is needed on the part of providers to assist enterprises in managing the myriad of security issues. From governance and compliance to operations, cloud providers have an obligation to lean towards greater disclosure of their activities, while preserving privacy obligations.

Cloud provider security is uneven overall, with some providers having excellent security programs and others leaving much to be desired. We must insist upon an industry standard baseline of security for all cloud providers, and we must insist upon a high level of transparency on the part of cloud providers as to their security efforts. Both enterprises and cloud providers need to work together to better align their security programs, architectures and communications.

CLOUD PROVIDERS MUST MAKE COOPERATION A PRIORITY

As with many young industries, cloud computing is hyper-competitive. This drive to excel in a new market can diminish and complicate efforts to collaborate with competitors. This can run counter to the interests of cloud consumers. In the long run, the cloud market will expand to greater levels if customers have confidence that cloud providers are working together to solve issues towards enhancing the “greater good” of the industry. Security assurance is of paramount concern when we discuss the greater good of the cloud computing industry.

Among the areas of cooperation and collaboration we feel are important include:

- Threat intelligence and incident sharing
- Transparency that extends assurances to verifiable controls with strong integrity checks
- Open interoperable standards development on common security requirements/controls
- Support for multi-vendor enterprise architectures to assure interoperability, data portability and vendor lock-in avoidance

Cloud providers need to put a greater emphasis on cooperation with their competitors to create greater trust in the industry and to accelerate security solutions.

CLOUD IS CHANGING THE VERY NATURE OF INFORMATION SECURITY

The rise of virtually unlimited compute and rapid instantiation of cloud services is inspiring new solutions to old security problems. Moving from servers that operate in a static fashion for years to services that may have a lifetime measured in seconds is among the characteristics of the new cloud world. Some researchers have described this phenomenon as taking a DevOps approach to information security. A focus on greater automation, disposable infrastructure, agility among other concepts are changing how we deal with problems such as malware, forensics, denial of service attacks and compliance.

At the same time, cloud computing does not exist in a vacuum. Complementary innovations such as Mobile Computing, Internet of Things, Software Defined Networks, Big Data and Artificial Intelligence must be understood and integrated into our cloud strategies and frameworks. The often conservative nature of information security favors clinging to best practices that we understand, but have diminishing value.

We need to take a hard look at many of our existing security practices and retire them in favor of new "cloud inspired" approaches that offer higher levels of security.

NATIONAL, REGIONAL AND INDUSTRY-SPECIFIC REGULATIONS PROVIDE IMPORTANT CHALLENGES

The myriad of regulations that touch upon information security are a significant challenge for the cloud provider and enterprise alike. Coping with compliance is a permanent part of the IT landscape, but we can make it better. This requires a clear view of the issues:

- Policies rapidly outdated by technology changes
- Duplicative nature of many regulations
- Conflicting regulations
- Global nature of enterprises and cloud providers vs regional regulatory authorities
- Knowledge gaps for regulators and auditors in addressing cloud computing

There are great opportunities in getting regulatory authorities to leverage existing regulations and standards, enter into mutual recognition schemes and other activities that drive the needed assurance without reinventing the wheel.

The regulatory environment, combined with the elastic and dynamic nature of cloud computing require a radical shift in compliance monitoring to reflect real-time activities. Legacy static "snapshot" type compliance monitoring has to be replaced with continuous compliance monitoring tailored to the cloud services being consumed.

It is critical that information security and privacy practitioners increase the scope and intensity of their collaboration to enhance regulatory outcomes that are optimized for both disciplines.

Our industry needs to engage with policy makers, regulatory bodies and their enforcement arms forcefully to help them understand cloud, where risks really lie and solutions that adhere to the spirit of the regulations.

INDUSTRY SKILLS GAP

Several studies estimate there are at least one million unfilled cybersecurity jobs[4]. A lack of qualified applicants is the primary reason for this gap. Among the information security professionals that are employed, they face tremendous challenges in keeping their skills current in the face of the accelerating pace of change catalyzed by cloud that is changing the security industry around them. Our security

[4] Forbes, One Million Cybersecurity Job Openings In 2016
http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/

education ecosystem needs to be greatly expanded, which will enhance the opportunities for today's security industry professionals.

We need to focus on generating more qualified professionals in the information security field and improving the skillsets of the existing professionals in particular around cloud technologies.

SUMMARY

Cloud computing is already making a tremendous impact on the IT landscape in its early years and has even greater promise for the future. This paper has outlined our view of the current state of cloud security and the issues that are holding it back from becoming a much larger and more beneficial industry. Insisting upon pervasive cloud security baselines, provider transparency, provider cooperation and managing inefficient regulations are among key issues of concern we have highlighted. We also discussed the need to understand how cloud is transforming information security and the formidable skills gap we have in this industry.

Enterprise consumers of cloud computing often seek to participate in solving these problems individually and quietly. With this paper, we are issuing a call to action to our industry peers to work with us on comprehensive solutions, and to engage with the information security and cloud computing industries as a community to deliver a more secure, resilient and trusted cloud for the benefit of all.

ABOUT THE CLOUD SECURITY ALLIANCE

The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

www.cloudsecurityalliance.org