May 12, 2015

Weil

Alert
Cybersecurity, Data Privacy & Information Management

One "Giant Leap" to a Secure Cloud Platform For U.S. Corporations

*By Paul Ferrillo, Jeffrey Osterman, and Grady Summers**

It is fitting that just over 40 years after Neil Armstrong walked on the moon and uttered some of the most famous words ever spoken, "one small step for [a] man, one giant leap for mankind," NASA, along with cloud service provider Rackspace, jointly launched an open-source cloud-software initiative known as OpenStack. The OpenStack project is intended to help organizations manage cloud-computing resources running on standard hardware. The early code came from NASA's Nebula platform as well as from Rackspace's Cloud Files platform. Launched with the intent to provide consumers with a high tech, yet low-cost method to store vast amounts of data off premises in a safe and efficient manner, the cloud has transformed the way global enterprises do business.[1] Yet, despite the cloud's increasing popularity, hardly a day goes by when industry professionals do not question the security of data kept in the cloud. According to Gilad Parann-Nissany, CEO and co-founder of cloud encryption company Porticor (recently acquired by Intuit):

> In the cloud, data security poses new risks and challenges. We are no longer concerned just with burglars breaking into our offices to steal computers, but rather with the data belonging to complete systems deployed to the cloud...Instead, security in the cloud becomes not about protecting our hardware, but rather protecting the sensitive information regardless of its physical location. For this, burglar alarms are irrelevant and firewalls are only one part of the approach for security in the cloud.
>
> A way to visualize the unique challenges of data security in the cloud is that where before we had brick walls and steel locks to keep us safe; we now must construct mathematical walls as barriers to our data.[2]

As more and more businesses are considering moving some or all of their data storage needs to the cloud, here are three "50,000 foot" questions American businesses and boards of directors are asking themselves (or should be asking their IT security professionals) before adopting a cloud-based strategy:

- How can the board assure itself from a governance perspective that the cloud-based environment that it is being asked to approve is acceptably secure, as compared with the company's previous on-site computer environment, and meets the security, privacy, and regulatory needs of my company?[3]

*Grady Summers serves as SVP, Cloud Analytics at Mandiant/FireEye.

- What visibility and ability does the company have if there is a cloud-based breach and its information is subject to exfiltration? Does the company have the ability to conduct incident response and remediation or is it totally at the mercy of the cloud service provider (CSP)?[4]
- What is the "best" way to assure that the company's cloud-based data is as secure as possible given what it knows about the CSP that it has chosen?

90% of All Organizations Have Security Concerns about the Cloud

A recent study noted that "an overwhelming majority of 90% of organizations are very or moderately concerned about public cloud security. Today security is the single biggest factor holding back faster adoption of cloud computing."[5] The Cloud Security report notes that the top concerns are:

- General security concerns over the storage of data in the cloud;
- Data loss and leakage risks;
- Loss of control over security procedures applied day to day over the company's data; and
- Lack of visibility to assure regulatory compliance.[6]

How would these concerns potentially materialize? Our experience tells us that, to the extent attackers are targeting data in cloud-hosted environments, they're doing it in distinctly old-fashioned ways. That is, despite concerns about the cloud being inherently insecure, attackers are using the same methods to compromise cloud resources as they have used for many years for on-site computer systems: the theft of employee credentials generally started via spear phishing attacks. Thus, we recommend that organizations approach cloud security like they would any other environment: by understanding their data and the threats against it, and ensuring that the environment is instrumented to prevent, detect, and respond to attacks. This can be hard, though, when IT security teams lack the necessary visibility to do their jobs.

This lack of visibility was illustrated in a recent Ponemon study entitled "The Cloud Multiplier Effect." The study, based on a survey of 613 IT and security professionals, found that increasing use of cloud services can increase the probability of a $20 million data breach by as much as 3 times. It also revealed other key findings, including:

- 36 percent of business-critical applications are housed in the cloud, yet IT isn't aware of nearly half of them;
- 66 percent of respondents believe that their organizations' use of the cloud diminishes their ability to protect sensitive or confidential information; and
- 72 percent of respondents don't believe that their cloud service provider would notify them immediately if they had a data breach involving the loss or theft of their intellectual property or business confidential information.[7]

Cloud-related breaches in 2014 included Dropbox, Google Drive, and the alleged Apple iCloud breach. More recently, SendGrid, the cloud email service, reported it had been hacked through a phishing scheme that compromised an employee's account.[8] Certainly these high-profile breaches, such as Dropbox (from which 7 million passwords were reportedly stolen) have left many questioning whether the cloud can be safely used to store sensitive data.

Types of Cloud Computing

We refer generally to "cloud computing," but this can refer to anything from a hosted application to rented servers in a shared facility. It is helpful to recognize the three major categories of cloud computing:

- **Infrastructure as a Service (IaaS):** In this model, the CSP is responsible for basic IT resources (servers) and the networks on which they run. The customer is generally responsible for maintaining the operating systems and software necessary to run the applications, plus the data placed in the cloud environment. Thus, while the CSP is responsible for protecting the infrastructure itself, data security in an IaaS environment is generally the responsibility of the customer.

- **Platform as a Service (PaaS):** Here the CSP provides the infrastructure, the operating system, and a set of services that organizations use to build applications. These building blocks are invoked through Application Programming Interfaces (APIs) and might include services for storage, databases, data processing, machine learning, etc. The customer is responsible for application deployment, and responsibility for security is generally shared between the customer and the CSP.
- **Software as a Service (SaaS):** Here the CSP provides for nearly everything, including the infrastructure and software provided to the customer. Thus, security in an SaaS environment generally is the responsibility of the provider, and it is the consumer's role to ensure the CSP's security processes meet the security and compliance requirements of the customer's business.

Cloud Compliance, Security, and Visibility

As CSPs move "up the stack" to offer robust PaaS and SaaS services, they begin to shoulder more of the burden for securing their customers' data. However, it will always be the responsibility of the customer to ensure that its constituents' data is secure. Since a customer can't always directly participate in securing this data, it must ensure that the service contract, together with any associated statement of work and/or service level agreement (SLA) provided by the CSP meets its needs. The parameters of these contractual arrangements will usually include information about service availability, incident response definitions and services, breach response notifications and timing, technical compliance and vulnerability management, and log management and forensic capabilities, together with an allocation of liability if these standards are not achieved.

While we have found that most large CSPs do an outstanding job of securing their environments – and dedicate tremendous resources to this task – all of the above categories of services must be described in generalities, meaning "here's how they generally work." The proof is really in the terms and conditions of the contractual commitments that the CSP agrees to make, and the sad fact is that many cloud service customers do not understand the value of substantive contracts with detailed terms relating to security.

Here are the most important issues to consider when contemplating a migration of important data to the cloud under an SLA:

- Breach and incident response – Cloud customers must understand how the CSP defines events of interest vs. security incident, what events/incidents the CSP reports to the cloud customer, and in which way. Customers should understand when and how quickly they will be notified if the CSP: suffers a breach, what information will they will be given by the CSP to help analyze the incident, will they have the opportunity (given the potential SLA in place) to participate in the incident response process, and will they be given the opportunity to contact and interact with the CSP's own incident response team?
- Where is the customer's data going to be "stored"? This is probably one of the most important questions for a customer, both from a legal perspective (meaning under what circumstances can data be subpoenaed or accessed through a court request or judicial process) and a privacy perspective (meaning how must data, such as personally identifiably information, be stored and protected).
- Does the CSP itself adhere to any standardized security practice or protocol, like the NIST cybersecurity framework, or ISO 27001? Does the CSP have FedRamp certification or a certification from the Security Trust and Assurance Registry certification program?
- Does the customer have the ability to audit or independently assess the security provided by its CSP to make sure the provider is compliant with various legal, industry, customer and regulatory requirements it may be subject to?
- What is the CSP's patch management process in case software or application vulnerability is discovered, which could then impact the security of the data stored?

- What sort of back up procedures does the CSP have in place if the customer's data is lost, stolen or deleted?

Thinking About Making a Move to the Cloud? Cloud Security Checklist

There is no perfect checklist of how, when, and where to move data to a cloud-based environment. Some factors, such as cost, may make the decision easy, while on the other hand, the perceived lack of control over your data security or your compliance risks may make the decision harder. At the end of the day, it is your business judgement what sort of data you are comfortable moving to the cloud (you might be comfortable moving human resources, payroll, or other specific applications[9]), and what sort of data you are not comfortable moving to the cloud (you might draw the line at PII or financial records and information). A separate book alone could be written on this sort of balancing act.

From a data security perspective, though, there are certain security measures that should be investigated by potential cloud customers before they make the decision to move their data to a cloud-based environment. This area is highly technical (and thus security professionals and cyber-governance and cybersecurity lawyers should also be consulted before making this decision), but we try below to boil down these measures into objectives for directors and officers to consider when asked to finally approve a move to the cloud:

- How is security built into the cloud architecture and applications and data that are going to be moved to the cloud-based environment? Is there a constant lifecycle of updates and vulnerability reviews given that the computing ecosystem is never static?
- What data am I putting in the cloud? Is it general company HR data, customer PII, financial records, or something else less sensitive?
- Will the data stored in the cloud be encrypted while at rest or only when it is in motion to and from the cloud? What sort of encryption is available at my CSP?
- How is suspicious activity monitored on the cloud? By the CSP only, or will the customer have visibility into security monitoring? Will cloud security be continuously monitored by the CSP?
- What degree of visibility does the CSP make available to the customer (audit logs and metadata recording administrative changes, account usage, system logs, etc.), and can this data be flexibly consumed into your own internal security monitoring systems?
- What sorts of intrusion detection systems are in place to detect threats to the cloud-based environment, such as malware threats, or suspicious network traffic?

So You Are Moving to the Cloud – Governance Issues Ultimately Rule the Day

This article is not meant to dissuade a company from considering using the cloud to increase efficiency in its businesses. On the contrary, our goal is to allow readers to engage in more informed discussions that will ultimately lead to a greater degree of comfort with both the decision to move to the cloud and the risk management tools, procedures, and contractual protections surrounding that move.

The cloud undoubtedly provides businesses with unique opportunities to manage their data in not only a cost efficient manner, but also potentially in a manner which is just as safe and secure as on-site storage systems. The cloud is not, however, a binary solution to data management challenges. And time is slim to consider all the options. Whatever the path you choose, you should consider how things may look at the end of the day if your company is breached, and some constituency (i.e., a regulator, state AG, or investor) looks back to potentially criticize your decision to move to the cloud. Have your checklists answered, discuss the answers to your checklists with your IT staff and outside experts, and document your decisions that balance the business and efficiency needs of the company with the level of security and service being offered by your cloud service provider.

1. *See* "The next generation of cloud computing," available at http://www.pwc.com/en_US/us/increasing-it-effectiveness/assets/next-generation-cloud-computing.pdf (noting "Cloud computing is the fastest-growing trend in enterprise technology today – and for the foreseeable future. Forrester Research predicts the global cloud computing market will mushroom from $40.7 billion this year to $241 billion by 2020.").
2. *See* "Cloud Computing Issues and Challenges," available at http://www.porticor.com/2014/11/cloud-computing-security-issues-and-challenges/.
3. "Compliance (64%) was seen as the biggest cloud security challenge," according to one recent report issued by CipherCloud. *See* "Compliance remains the key cloud security challenge, according to the CipherCloud report," available at http://www.cloudcomputing-news.net/news/2015/mar/26/compliance-remains-key-cloud-security-challenge-according-ciphercloud-report/.
4. *See* "Majority of firms say they aren't confident in responding to cloud-based data threats," available at http://www.cloudcomputing-news.net/news/2015/apr/08/majority-firms-say-they-arent-confident-responding-cloud-based-data-threats/ (noting that 60% of the global respondents in a recent survey were not confident they had the ability to proactively respond to cloud-based data threats).
5. *See* "Cloud Security Spotlight Report," available at http://www.infosecbuddy.com/wp-content/uploads/2015/03/Cloud-Security-Spotlight-Report-2015.pdf (hereinafter, the Cloud Security Report).
6. *Id.*
7. *See* "The Cloud Multiplier Effect on Data Breaches," available at https://blog.cloudsecurityalliance.org/2014/06/04/the-cloud-multiplier-effect-on-data-breaches/.
8. *See* "SendGrid admits hack, says all customers must reset their passwords," available at http://venturebeat.com/2015/04/28/sendgrid-admits-hack-says-all-customers-must-reset-their-passwords/.
9. *See* "Navigating security in the cloud," available at http://www.pwc.com/en_US/us/it-risk-security/assets/pwc-navigating-security-in-cloud.pdf.

Cybersecurity, Data Privacy & Information Management is published by Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

If you have questions concerning the contents of this issue, or would like more information about Weil's Cybersecurity, Data Privacy & Information Management practice, please speak to your regular contact at Weil, or to the editors or authors listed below:

Editors:

Michael Epstein (NY)	Bio Page	michael.epstein@weil.com	+1 212 310 8432
Randi Singer (NY)	Bio Page	randi.singer@weil.com	+1 212 310 8152
Paul Ferrillo (NY)	Bio Page	paul.ferrillo@weil.com	+1 212 310 8372

Contributing Authors:

Paul Ferrillo (NY)	Bio Page	paul.ferrillo@weil.com	+1 212 310 8372
Jeffrey Osterman (NY)	Bio Page	jeffrey.osterman@weil.com	+1 212 310 8155