In Search of a Strategy for Security in the Cloud

Eduardo Correia
Ara Institute of Canterbury
eddie.correia@ara.ac.nz

Bernard Otinpong
Ara Institute of Canterbury
bernard.otinpong@ara.ac.nz

ABSTRACT

In the public cloud responsibility for security is shared between the organisation and the cloud service provider (CSP). Exactly how these responsibilities are assigned, what is referred to as the "trust boundary," depends on the service level agreement (SLA), the capability of the provider and the service delivery model. As the traditional approaches to security no longer apply, this has given rise, in industry, to a certain lack of clarity, even confusion. This paper, through the use of a systematic review, assesses a number of strategies and frameworks that integrate security in cloud solutions and deployments, and identifies one particularly useful and flexible framework that organisations can use in the cloud.

Keywords: Security, Service Level Agreement, SLA, Cloud Computing, Cloud Service Provider, NIST, Cybersecurity, Framework, Trust Boundary

1. INTRODUCTION

There is no single approach to security in the public cloud. At this stage, while a great deal has been written about it, no consensus has yet emerged. Scholars and practitioners have proposed a whole range of approaches to making security an integral part of solutions and deployments in the cloud, resulting, at times, in a profound lack of clarity on the matter. The reality is that differences do exist between traditional on premise environments and the public cloud with its widespread use of multitenancy, the existence of a trust boundary and the critical role of the service level agreement (SLA).

The paper therefore considers security in the context of not just the cloud as we know it but more specifically the nature of shared responsibility for security. This factor is most clearly captured in the trust boundary, which defines each party's set of responsibilities for security. It then looks at each strategy in terms of its usefulness to small and medium sized businesses, with the aim of finding one that is simple and straightforward enough to guide security in the cloud but comprehensive enough to provide effective protection on a wide range of issues facing business.

2. BACKGROUND

Security is a major factor in moving workloads to the cloud. Surveys show this as a serious challenge, not just in the early days of the cloud (Gens, 2009) but all the way through to the present. Roughly three quarters of people managing their organisations' cloud security being nervous about the security of applications and data in the public cloud (Forrester, 2015), and these concerns are reasonable. The Zeus botnet originated from an EC2 web site in AWS, and while AWS consistently insist that customers secure workloads and approach IaaS as they would their demilitarized zone (DMZ), the reality is that variants of Zeus are believed to have resulted in the loss of some $100 million from bank accounts in 2009 (Babcock, 2010). Code Spaces, a company that made use of the AWS platform, went out of business due to a single cyber-attack, not because their servers in the cloud were compromised but because the intruder took control of the AWS control panel or possibly a system that hosted the tools (e.g. an administrator's workstation) (Nunnikhoven, 2014). Another concern is the risk that government and law enforcement agencies can more easily get to the data (Velte, Velte, & Elsenpeter, 2010). The USA Patriot Act gave the U.S. government the ability to request data from U.S. based companies, even if the data was stored in another country. There are many other examples. In fact, in 2016 there were almost 1.4 billion data security breaches (Gemalto, 2017). (Interestingly only 4.2 % involved data that was encrypted (Gemalto, 2017).)

This situation is exacerbated by widespread deficiencies in understanding of the fundamentals of security, even among people who should know better. Rittinghouse & Ransome (2009) for instance claim that data in the public cloud "leaves organizations open to large distributed threats" and that "attackers no longer have to come onto the premises to steal data." As the practitioners know, once on premise infrastructure is connected to the internet, data can be stolen and compromised through that connection and that someone does not need to be on the premises and this is not exclusively found in cloud deployments.

Major industry players are also responsible for some of the confusion. Rik Fairlie (2011, March 15), for instance, in an effort to promote Microsoft's private cloud solution, argued that the "security, compliance, and availability of public cloud computing have dissuaded many CIOs from sending critical applications and data to the cloud." Then two weeks later argued that as the public cloud was considered secure enough for the US military, it should be secure enough for any civilian organisation (Fairlie, 2011, March 29).

3. METHOD

Since cloud computing can still be considered a recent development, one that is constantly changing, it can be difficult to find relevant recent sources. A systematic literature review was made from secondary resources, mainly acknowledged texts, standards documents, industry periodicals and white papers, analysts' reports and conference journals. The review of literature was from 2008-2017, because the term cloud computing was popularly used only after 2008, so the literature review focuses on studies published after that year. The literature review process followed steps for conducting a review as suggested by (Oates, 2005). The seven steps include: searching, obtaining, assessing, reading, critical evaluation, recording, and writing critical review.

It is the nature of the data that determines the level of security that is required (Kavis, 2014). For instance, health care or financial data typically requires a higher level of security than

This quality assured paper appeared at the 8th annual conference of Computing and Information Technology Research and Education New Zealand (CITRENZ2017) and the 30h Annual Conference of the National Advisory Committee on Computing Qualifications, Napier, New Zealand, October, 2-4, 2017. Executive Editor: Emre Erturk. Associate Editors: Kathryn MacCallum and David Skelton.

online gaming. Security does need to be highly specified in the case of data and systems that have higher levels of requirements. In these cases use is made of security service level agreements (secSLAs). Cloud service providers (CSPs) take matters of compliance seriously, whether it be government regulations such as the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), or industry standards such as the PCI DSS. Government policy makers face not just rapid change but the acceleration of rapid change in the cloud computing. This includes the data being held by CSPs in foreign countries, while facing the challenges of data sovereignty and privacy. As much as compliance and regulation is important, this falls outside the scope of this paper.

This literature review paints a picture of how systems, data, resources and workloads in the cloud can be secured within the context of the trust boundary. It involved selecting and analysing strategies and frameworks potentially useful for business on the basis of three basic criteria: they provide a broad conceptual framework, focus on practice, and are uncomplicated enough for practitioners to take them seriously. In short, strategy should lead to action.

4. THE TRUST BOUNDARY

The cloud reduces but does not eliminate the scope of security responsibilities (Riley, 2017). As the public cloud necessarily entails entrusting a substantial part of the network, systems, applications and data to a third party, the responsibility for security is no longer the exclusive domain of the organisation. It is instead shared between two or more parties: the CSP (or "provider"), the customer and sometimes also an application service provider. Each party's responsibilities are delineated by what is commonly referred to as the "trust boundary" and organisations need to understand exactly where that boundary is located. This boundary is defined by three factors: the service-level agreement (SLA), the service delivery model (SPI) and the capabilities of the CSP (Mather, Kumaraswamy, & Latif, 2009, p.110).

In the case of Infrastructure as a Service (IaaS), the provider is responsible securing only physical infrastructure and the underlying hypervisor. Special precautions need to be taken because different organisations using the same provider make use of the same infrastructure and systems as other organisations, a key factor that drives down the cost of cloud services. The responsibility for keeping the data and systems of tenants apart, though, is always the responsibility of the CSP. The customers are responsible within deployments for the operating system, for instance patch management, and need to ensure that their architecture have further separation of systems and applications, and that these adhere to the auditing and certification necessary for compliance (Riley, 2017).)

As one moves up the stack, the trust boundary shifts and the provider accepts progressively more security responsibilities. Platform as a Service (PaaS) entails entrusting the cloud provider with all the security associated with IaaS but also, in addition, the operating systems and associated maintenance, so that patch management of the operating system, unlike in the case of IaaS, is not the responsibility of the customer but that of the provider. The customer is then left with the job of securing the applications, both in terms of how they are written, configured, deployed, maintained and utilised (Gurkok, 2017).

This still leaves a great deal of responsibility for security with the customer, especially as applications have been identified as especially vulnerable because they contain so many lines of code, with different programmers of different skill levels using a variety of programming languages, which themselves could contain vulnerabilities (Singh et al, 2016). CSPs therefore need to provide customers with the tools and services to implement intrusion detection and various forms of monitoring (Gurkok, 2017).

In the case of Software as a Service (SaaS), the provider is responsible for the security of the application but the customer's involvement is limited to provisioning users, assigning roles and so on. While the customers have fewer responsibilities in terms of SaaS, they must be familiar with the security measures and precautions of the vendor. In all cases, whether it be IaaS, PaaS or SaaS, customers are responsible for certain things. They are for instance responsible for Economic Denial of Service (EDoS), where an attacker manages to access the customer's account and then uses it or racks up huge costs on it.

The SLA, an essential component of cloud services, outlines the responsibilities of the cloud provider, including security. As cloud computing becomes more ubiquitous both public and private organisations struggle with the appropriateness of SLAs (Alhamad, Dillon, & Chang, 2010). These are seen by many as an instrument to help foster adoption and widespread acceptance of cloud computing, but at the same time are alleged to be ineffective, meaningless and costly to administer (Alhamad, Dillon, & Chang, 2010). This was emphasised by Durkee (2010) who stated that SLAs, when they are not properly defined and administered, fail to meet the expectations of businesses and could impede adoption. Further, Durkee stated that SLAs when executed by service providers are very optimistic and difficult to enforce. SLAs should ensure that a third party can review the metrics and compliance but providers do tend to subject themselves to frequent audits (Gurkok, 2017).

5. STRATEGIES FOR SECURITY

5.1 Security Classification

Hussain, Fatima, Saeed, Raza, & Shahzad (2017) provide a framework for levels of security attacks across different cloud services at different layers, which includes a ranking of risk categories of low, medium and high (Hussain, Fatima, Saeed, Raza, & Shahzad, 2017). These risks increase in severity in the lower levels of infrastructure and platform. The framework maps cloud services to security requirements and list security requirements as data encryption, multitenancy, authentication, and authorization. (Hussain, Fatima, Saeed, Raza, & Shahzad, 2017).

Hussain, Fatima, Saeed, Raza, & Shahzad (2017) consider within SaaS the following major security concerns: data protection, interfaces and Secure Shell (SSH). They then consider IaaS and PaaS together due to their being interdependent. In this area the security concerns are hardware virtualisation, software virtualisation, multitenancy and the nature of SLAs. The solution is to implement a "dynamic security contract to determine the risk level and type of security required for each service at different cloud layers" (Hussain, Fatima, Saeed, Raza, & Shahzad, 2017). As a strategy to security in the cloud, this multilevel classification lacks the kind of clarity and flexibility of two other major frameworks: the "AWS Cloud Adoption Framework" (Amazon Web Services, 2016) and the "Framework for Improving Critical Infrastructure Cybersecurity" (National Institute of Standards and Technology, 2017) or in fact even the work of cloud architects like Michael J. Kavis (2014).

5.2 Three-part Strategy

Kavis (2014) outlines a three-part security strategy of protection, detection and prevention. Protection involves making use of policies and processes to protect the organisation from breaches in security. Detection involves checking logs,

events and finding security vulnerabilities. Prevention involves taking the action necessary to prevent problems once something is detected. Some of the most important areas of focus in the cloud are policy enforcement, encryption, key management, web security, API management, patching and updating, logging, monitoring and auditing (Kavis, 2014). Kavis (2014) recommends that organisations focus on three core strategies for cloud-based applications: centralisation, standardisation and automation. By this he means that the approach to security involves the following:

- The controls, processes and services related to security should be managed centrally.
- The approach to security should be standardised across the organisation, rather than be specific to a particular situation or instance.
- Code should be used wherever possible so that activities are scalable and consistent.

The strengths of this approach is that it is practical and provides guidance for organisations wishing to move workloads to the cloud.

5.3 AWS Framework

In its "Security Perspective" of the "AWS Cloud Adoption Framework" (Amazon Web Services, 2016), Amazon Web Services (AWS) approach cloud security in the form of five security controls. These are:

- Identity and Access Management (IAM): the management and control of data and the access to it
- Detective Control (DC): native logging and services that provide visibility for what is happening
- Infrastructure security (IS): controls and ability to automate security infrastructure
- Data Protection (DP): management and control of data and the access to it
- Incident Response (IR): response to security incidents, including reducing harm and restoring operations

This approach is clearly delineated so that customers utilising the AWS cloud can distinguish between five major areas of security. Identity management as a service for authentication, authorisation, provisioning, auditing, often within the context of collaborative Meta systems is critically important and fundamental, especially in view of increasing levels of identity theft. In fact these thefts account for 54% of all data breaches and one third of the most severe data breaches (Gemaldo, 2014).

The one factor missing in the AWS strategy is what Singh, Jeong, & Park (2016) call "trust and conviction." This term refers to everything from SLAs and compliance, both internal and external, through to perceptions of cloud security and matters of a more philosophical nature. To some extent this omission is understandable, as the AWS approach shows a bias for action, and is predicated on the changes to the Software Development Life Cycle (SDLC), with applications changing far more quickly, so increasing the risk of breaches in security. Its principal weakness is that this framework reflects vendor bias and while it is widely applicable, may not work as well with other platforms.

5.4 NIST Framework

Perhaps the most comprehensive and flexible strategy for organisations to adopt is the "Framework for Improving Critical Infrastructure Cybersecurity" (National Institute of Standards and Technology, 2017). The National Institute of Standards and Technology (NIST) framework, still in draft form, comprises of three basic components:

- The framework core. The cybersecurity activities, outcomes and references common to infrastructure. These include the division of security into five parts (or "functions"): identify, protect, detect, respond and recover. These functions are subdivided into "categories," which are closely linked to specific activities, such as "Asset Management," "Access Control" and "Detection Processes." These are accompanied by "Informative References," which provide guidance for achieving certain outcomes.
- The framework implementation tiers. This refers to an organisation's security practices and the rigor and sophistication of how it manages risk, and this includes a wide range of cybersecurity factors, which are informed by business needs. This involves organisations making use of various external sources, including those of U.S. government departments. Four tiers exist, each defining progressively improved levels of performance in terms of security, starting with Tier 1 (Partial) to ending in Tier 4 (Adaptive).
- A framework profile. These are Framework categories and subcategories selected based on business needs for the desired outcomes. In this way the organisation is able to align cybersecurity with business requirements, risk tolerance and resources available. Different organisations will have different framework profiles.

Both AWS and Microsoft are taking the NIST Cybersecurity Framework seriously and supporting it. The framework guides government policy and activities in the United States, particularly in terms of the requirements in the government clouds (Amazon Web Services, 2017). Microsoft have even integrated the NIST framework into their enterprise risk management programme (Nicholas, 2017).

One increasingly common approach is to outsource security entirely through the use of managed security services (MSSs). Often organisations are not easily able to provide 24X7 network security, such as firewalls or intrusion detection systems, and so consider outsource their information security. This can be an independent third party or the CSP but essentially these vendors share their expertise, tools and resources with their customers.

6. CONCLUSION

Over the past 10 years or so, attitudes to security in the cloud has changed. While some people continue to be concerned, the truth is that trust in the sector is growing and concerns about security diminishing (Rightscale, 2017, Panko, 2017). It is clear that security is no longer a serious impediment to the adoption of cloud in most organisations, with rapid growth in this sector of the industry. Security in the cloud is perceived to have improved. These days all major CSPs have what Velte, Velte, & Elsenpeter (2010) call "extensive security controls." The cloud is no longer novel, and whereas previously compliance standards were not designed with the cloud in mind (Rittinghouse & Ransome, 2009), now they are.

In some ways the cloud makes security easier for organisations. While the public cloud, by definition, involves losing direct control over physical infrastructure, hypervisor and other software, most practitioners acknowledge that AWS, Microsoft

and other providers offer customers a wide range of tools and expertise to secure technologies and services available on their platforms. Furthermore, the major providers are better placed than most organisations to deal with a range of cyber-attacks such as DDoS, and take security seriously. They provide platforms that are secure by default, for instance make use of security groups that act as a firewall so customers can choose which protocols and ports are open to computers over the internet. While the cloud has resulted in ever greater levels of centralisation, making them arguably easier to target, this does have advantages. It can for instance reduce data loss on laptops that are misplaced or stolen, and make the remote management of devices easier and organisations can employ advanced logging techniques (Velte, Velte, & Elsenpeter, 2010, p.38).

A major concern is the shortage of knowledge and skills in cloud computing. At this point, it is still unclear how capable technical staff of most corporations are in terms of building not just solutions but secure solutions in the public cloud. It might well be that the provider platform is secure but the implementation of the solution on that platform is anything but secure. This factor is, according to one credible source, currently inhibiting the adoption of cloud services (Intel Security, 2017) and something that institutes and universities here in New Zealand and elsewhere should do something about.

7. REFERENCES

Alhamad, M., Dillon, T., & Chang, E. (2010, April). Conceptual SLA framework for cloud computing. In Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference on (pp. 606-610). IEEE.

Amazon Web Services. (2016, June). AWS Cloud Adoption Framework: Security perspective. Retrieved from https://d0.awsstatic.com/whitepapers/AWS_CAF_Security_Perspective.pdf

Amazon Web Services. (2017). NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS cloud. Retrieved from https://d0.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf

Babcock, C. (2010). Management strategies for the cloud revolution. New York: McGraw Hill.

Durkee, D. (2010). Why cloud computing will never be free. Communications of the ACM, 53(5), 62-69.

Fairlie, R. (2011, March 15). Top 5 questions CIOs should ask private cloud vendors. Retrieved from https://www.forbes.com/sites/microsoft/2011/03/15/top-5-questions-cios-should-ask-private-cloud-vendors/#5acde5fc3b26

Fairlie, R. (2011, March 29). Cloud is secure enough for the Pentagon. Why not you?. Retrieved from https://www.forbes.com/sites/microsoft/2011/03/29/cloud-is-secure-enough-for-the-pentagon-why-not-you/#5703c48e3faa

Forrester Consulting (2015). Best practices for public cloud security. Retrieved from https://www.trendmicro.com/aws/wp-content/uploads/2015/12/Cloud_Security-Part3-Forrester_Best_Practices_Whitepaper-Feb2015.pdf

Gemalto (2017). Mining for database gold: Findings fromt eh 2016 Breach Level Index. Retrieved from http://www.breachlevelindex.com/assets/Breach-Level-Index-Report-2016-Gemalto.pdf

Gens, F. (2009, December 15). New IDC IT Cloud Services Survey: Top Benefits and Challenges [Blog post]. Retrieved from http://blogs.idc.com/ie/?p=730

Gurkok, C. (2017). Securing network security. In J. Vacca (Ed.) Computer and Information Security Handbook. Third Edition. Cambridge, MA: Morgan Kaufmann.(http://www.sciencedirect.com/science/article/pii/B9780128038437120010) (pp.83-126). Waltham, MA: Elsevier.

Hussain, S.A., Fatima, M., Saeed, A., Raza, I., & Shahzad, R.K. (2017). Multilevel classification of security concerns in cloud computing. Applied Computing and Informatics, 13, 57-65.

Intel Security. (2017). Building trust in a cloudy sky: the state of cloud adoption and security. Retrieved from https://www.mcafee.com/us/resources/reports/rp-building-trust-cloudy-sky.pdf

Kavis, M. J. (2014). Architecting the cloud: Design decisions for cloud computing service models (SaaS, PaaS, and IaaS). Hoboken, N. J.: John Wiley & Sons.

Mather, T., Kumaraswamy, S., & Latif, S., 2009. Cloud security and privacy. Sabastopol, CA: O'Reilly.

National Institute of Standards and Technology (2017). Framework for Improving Critical Infrastructure Cybersecurity. Draft version 1.1. Retrieved from https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf

Nicholas, P. (2017, June 7). NIST Cybersecurity Framework: Building on a foundation everyone should learn from [Blog post]. Retrieved from https://blogs.microsoft.com/microsoftsecure/2017/06/07/nist-cybersecurity-framework-building-on-a-foundation-everyone-should-learn-from

Nunnikhoven, M. (2014). The Code Spaces nightmare. Blog, retrieved from http://blog.trendmicro.com/the-code-spaces-nightmare

Oates, B. J. (2005). Researching information systems and computing. Sage.

Panko, R. (2017). The cloud in 2017: Trends in security. Retrieved from https://clutch.co/cloud/resources/annual-cloud-computing-survey-2017

Rightscale (2017). State of the cloud report. Retrieved from http://assets.rightscale.com/uploads/pdfs/RightScale-2017-State-of-the-Cloud-Report.pdf

Riley, S. (2017, May 8). Staying secure in the cloud is a shared responsibility. Gartner database. Retrieved from https://www.gartner.com/document/3277620?ref=solrAll&refval=188615362&qid=783e927cdc453bce50a7ac781aeece18

Rittinghouse, J.W. & Ransome, J.F. (2009). Cloud computing: Implementation, management, and security. Boca Raton, FL: CRC Press.

Singh, S., Jeong, Y, & Park, J.H. (2016). A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications. 75, 200-222.

Velte, A.T., Velte, T.J., & Elsenpeter, R. (2010). Cloud computing: a practical approach. New York: McGraw Hill.