Improving Cyber Security with the Cloud

(White Paper)

Executive Summary

Cloud computing has been touted the fifth generation of computing after the Internet. This new phenomenon brings with it unprecedented opportunities for organizations to grow their digital assets securely and reliably. First, cloud computing systems can leverage on economies of scale to boost their security mechanisms at a fraction of traditional costs. And with organizations (the domain experts) and technology providers coming together to form a closely-weaved cloud ecosystem, it becomes easier for everyone to stay relevant amidst dynamic cyber threats. Finally, moving critical computational tasks to the cloud also helps to eliminate the threat of physical theft and loss. That said, it is undeniable that cloud computing does have its share of security challenges. The good news is that many cloud service providers have taken considerable measures against these challenges. For instance, encryption has been used to protect the transmission and storage of confidential information across cloud systems.

Background

Cloud computing has often been regarded as a "dream come true" for businesses. Newfound agility, productivity and scalability at a fraction of traditional costs are but a few benefits on the list. (The Open Group, n.d.) With over 90% of businesses surveyed adopting cloud technologies in 2015 (Weins, 2015), it is of no surprise that this market is expected to grow at a compound annual growth rate (CAGR) of 19.62% in the next three years, and hitting $43B by 2018. (Columbus, 2015)

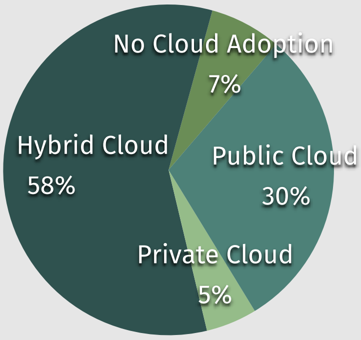
Moving to the Cloud: New Opportunities or New Threats?

It is not all rosy for organizations though. The rise of cloud computing brings with it new challenges and risks that many organizations are having a hard time combating, mostly due to the lack of skilled talent and experience. One of which is cyber security; specifically, security challenges pertaining to cloud computing systems (hereinafter referred to as "cloud systems").

In a recent study released by Rackspace, businesses highlighted security concerns such as "meeting security requirements" (48%) and "losing control of data to a third party provider" (39%) as their top considerations in migrating to cloud systems. (Bourne, 2016)

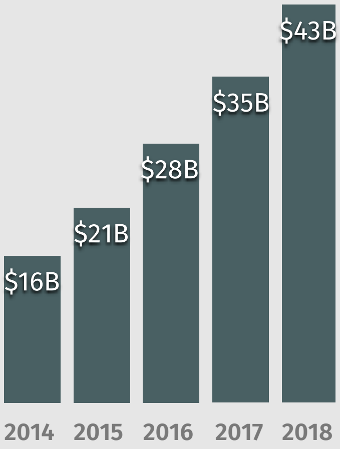
But let's not forget that traditional IT systems are not without vulnerabilities. What organizations often neglect is - cloud technologies have advanced to a point where they could provide far more security and resilience than their on-premise counterparts (and oftentimes at a lower cost too). In a 2014 study compiled by Privacy Rights Clearinghouse, out of the 155 data violations relating to hacking and malware, only an estimated 10% occurred in cloud systems. The large majority of the cases affected on-premise and other proprietary systems. (Engates, 2015)

Cloud adoption in enterprises, out of 930 IT professionals surveyed



(Source: RightScale 2015 State of the Cloud Report)

Projections for cloud computing infrastructure and platform market



(Source: Goldman Sachs Research)

More IT experts are calling for the move to cloud systems (Jordan Times, 2012) and it is evident that the cloud is more than just a hype - it provides an unprecedented opportunity for organizations, big or small, to thrive securely and reliably.

Combating Cyber Attacks with the Cloud

Today and in the future to come, our world is increasingly digitized and automated with computer systems. The *Internet-of-Things* is one phenomenon epitomizing this trend. As these computer systems grow in volume and complexity, cyber attacks too have become more widespread, sophisticated and costly. A 2015 survey by PwC reported a 66% year-over-year increase in frequency of information security breaches reported since 2009. Financially, the average loss of these breaches also have also increased by 37% from 2013 to 2014. (White, 2014) Cyber attacks are no longer a question of *if* they will strike, but rather, *when* they will strike.

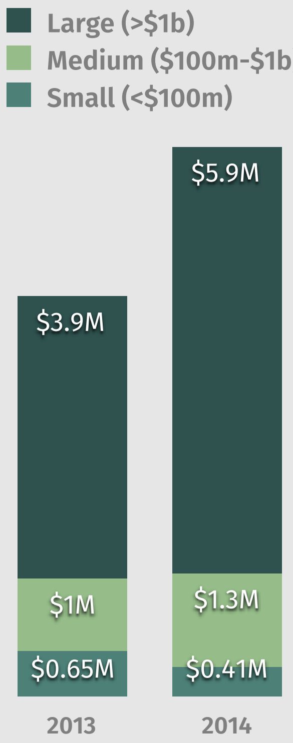
Yet, many organizations lack the expertise and resources necessary to tackle these imminent dangers in-house. This is one big driver for organizations to turn to the cloud as an effective remedy against cyber security vulnerabilities.

This section discusses three primary factors that enable cloud technologies to better protect IT systems from cyber attacks. These competitive advantages are what traditional IT systems have often been deprived of.

(A) Cloud platforms can do more with less

Most organizations that exist outside or along the perimeter of the technology domain regard IT as their cost or support center, and may not pay as much attention to it. Moreover, internal IT departments tend not to be bothered with competition or innovation, and hence may be handicapped

Average financial losses from security breaches, by company size (revenue)



(Source: Global State of Information Security Survey 2015)

in keeping up with the fast pace of technological advancements. On the other hand, cloud service providers are inherently technology companies. Their business survives on the technical talent and expertise they develop. Not to mention their strong innovation spirit that is essential to preserve their competitive advantage.

Coupled with the scale of operations that covers a large group of users, these cloud service providers can leverage on economies of scale to improve the efficiency and effectiveness of their security mechanisms at a fraction of the cost. (The Open Group, n.d.) For example, with a large and diverse problem-solution pool on hand, cloud platforms can effectively detect and counter anomalies or other signs of cyber attack across their client systems. Cloud providers also often offer redundancy in their systems, which duplicates critical information and processes across data centers to protect against downtime or losses due to on-site accidents. (Chia, 2012)

(B) The cloud ecosystem helps organizations stay relevant

Increasingly, experts are encouraging organizations to adopt a Cyber Threat Intelligence (CTI) approach in managing cyber security risks. This means identifying the attackers, understanding their motives and knowing how their attacks are executed. CTI enables organizations to transform from a reactive to a proactive stance, so that cyber attacks can be anticipated and prevented. (Henderson, 2015) A sophisticated approach like this requires timely analysis of external and internal intelligence, where organizations become constantly aware and alert of their surroundings. But it's easier said than done on a single-entity level due to the limited exposure and experience.

With the cloud, organizations and technology providers can come together to form an ecosystem that shares knowledge, expertise and experiences both on a domain-specific and technology level. (The Open Group, n.d.) The ecosystem can also further establish industry standards and formalize best practices to create a sustainable environment that supports security intelligence within and between organizations, old or new.

(C) Securing information on the cloud reduces the risk of physical theft and loss

For decades, organizations have had to manage the physical security of sensitive data that exists in physical (e.g. on paper) and electronic forms (e.g. in computers, laptops and electronic media). This is no easy feat as it involves both technology- and people-management. And when security is breached, even on an individual level, the cases can prove to become very costly. In 2002, an analyst from the U.S. Department of Veterans Affairs brought his laptop and hard disk off-site to work from home, and got them stolen. In this single case of theft, 26.5 million people had their Social Security numbers and other sensitive information leaked. (EPIC, n.d.)

Though users still access the cloud via their devices, cloud systems usually integrate multiple client authentication mechanisms that help to ensure the system is guarded against intrusion. More details are discussed in point (C) of the next section below. Moreover, cloud services usually require connection to the Internet, which brings the device online for remote access at real-time. For instance, the device owner can erase all device data remotely or even find the device with geolocation services.

> "Migrating data into the cloud is an excellent protection against data loss and key to ensuring data integrity. Accidental or malicious manipulation of data can occur very easily when data is kept locally, but virtually impossible on cloud services with access control and audit logs."
>
> **Jorg Haslbeck**
> Chief Technology Officer,
> Neuro10

Addressing the Challenges of Cloud Systems

Despite the newfound benefits of cloud systems discussed previously, it is undeniable that cloud technologies have inherent challenges that should never be neglected in the pursuit of security. Most cloud service providers recognize this concern and have placed security within their top priorities. Some of their claims have been backed with real tangible efforts that have tremendously enhanced the overall security of such cloud systems.

This section discusses three prominent security challenges of cloud systems that would likely be faced by organizations considering cloud adoption, as well as common practices that have helped overcome these challenges.

Responsible cloud service providers should minimally consider these factors in their implementation for good information security that promotes confidentiality, integrity and availability (also known as the CIA triad). Decision makers and users need to also be aware of the situation to make educated choices on their preferred cloud service provider.

(A) Releasing data externally may risk privacy issues

When using cloud services, users often have to release data to external systems that exist outside their corporate or private networks. The data transmission, storage and computational activities involved may pose as a threat to data privacy and confidentiality. This is especially critical for sensitive data that may even be governed by corporate policies or legal regulations.

Ways to overcome: The key here lies in the ability of the cloud system to protect critical data from being disclosed to unauthorized parties. One essential technology used widely for data confidentiality is encryption. (Chia, 2012)

Case Study: Neuro10's Encryption Technology

Cloud service provider Neuro10 offers its Big Data application via a SaaS model, where users can access the application remotely using a web browser over the Internet.

To safeguard user data, Neuro10 encrypts the data before transmission with its application agent (SecureForwarder) and also encrypts the transmission channel with the HTTPS protocol. SecureForwarder thus provides an additional layer of protection on top of HTTPS.

Encryption ensures that only authorized parties (with the correct key) can read the protected information. A popular application of encryption can be found in the HTTPS protocol (i.e. HTTP communication over SSL/TLS), which enables secure communication over the Internet. Cloud service providers should similarly encrypt sensitive communication channels and data stores.

(B) Moving into cloud introduces change to internal capabilities and processes

Cloud is a relatively new and radical technology to many organizations, especially those that do not deal with technology as their primary function. In terms of cyber security upon migrating to the cloud, organizations may or may not be prepared for the potential threats and mitigations. It takes time and effort to understand the technology, then adapt existing capabilities and processes to manage the risks involved.

Ways to overcome: Fortunately, organizations are not left alone. The cloud computing space has grown and diversified so much that numerous providers now exist to offer a variety of services. They collectively help to provide up-to-date, 360-degree solutions that meet the varied needs of users, including security needs. If managed well, cloud adoption could in fact help improve organizational agility, competence and security in the long run.

For instance, on-premise systems can easily integrate with third-party cloud platforms to form hybrid clouds, so that data storage and processing can be optimized on- and off-site. Some platforms also provide greater flexibility to users with virtualized environments that cater to different control levels, such as virtual machines with sandboxes and chroot jail. This allows users to exercise their control and discretion when necessary.

Case Study: Neuro10's RBAC Implementation

Neuro10's platform implements RBAC that categorizes users into two distinct hierarchical groups - *Admin* and *Normal* users. *Normal* users can only view data, while *Admin* users have additional edit and account rights (e.g. writing or deleting data). This implementation helps organizations to ensure that the right users are given the right access privileges at the right times.

(C) Remote access requires reliable electronic identities

Cloud systems enable ubiquitous computing, where computing becomes available anytime and anywhere to users. This means that users are able to access cloud services across multiple devices and platforms seamlessly. But such an implementation proves to be a huge security challenge for providers in identifying, authenticating and authorizing each access into the system. And if not managed properly, users may also suffer from poor platform usability or behave in a way that counteracts the security defenses (e.g. security may be compromised when users have too many passwords to remember and start jotting them down on paper).

Ways to overcome: Most cloud service providers have invested in developing reliable Identity and Access Management (IAM) capabilities that can ensure that the right users are granted appropriate access to the right resources at the right times. Role-Based Access Control (RBAC) is also often used in tandem with IAM to more efficiently manage user access since the appropriate usage rights are tagged to user roles instead of single requests. (PwC, 2014) This helps to streamline access control mechanisms for ease-of-management and improved usability.

Conclusion

The cloud computing space is still and will continue evolving. It is a continuous challenge for cloud service providers to stay abreast of security trends, but probably even more challenging for organizations who do not function at the forefront of technology. Instead, these parties should work hand-in-hand to synergize their domain and technical expertise in combating cyber security threats that are growing in size and complexity. If these threats are not well-managed, the whole technology landscape will stall and may even backfire on the parties involved.

References

The Open Group. (n.d.). Cloud Computing for Business : Why Cloud? Retrieved February 2016, from The Open Group: http://www.opengroup.org/cloud/cloud/cloud_for_business/why.htm

Weins, K. (2015, February 18). Cloud Computing Trends: 2015 State of the Cloud Survey. Retrieved February 2016, from Cloud Management Blog: http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2015-state-cloud-survey

Columbus, L. (2015, September 27). Roundup Of Cloud Computing Forecasts And Market Estimates Q3 Update, 2015. Retrieved February 2016, from Forbes: http://www.forbes.com/sites/louiscolumbus/2015/09/27/roundup-of-cloud-computing-forecasts-and-market-estimates-q3-update-2015/#3e9653166c7a

Bourne, J. (2016, January 6). How security will accelerate, not inhibit, cloud adoption in 2016. Retrieved February 2016, from CloudTech: http://www.cloudcomputing-news.net/news/2016/jan/06/how-security-will-accelerate-not-inhibit-cloud-adoption-2016/

Engates, J. (2015, December 16). Cloud Predictions for 2016. Retrieved February 2016, from Rackspace: http://blog.rackspace.com/cloud-predictions-2016-john-engates/

Jordan Times. (2012, June 19). IT experts advocate adoption of cloud computing. Retrieved February 2016, from TMC News: http://www.tmcnet.com/usubmit/2012/06/19/6381327.htm

White, S. (2014, October 8). Global cyber-attacks up 48% in 2014. Retrieved February 2016, from CGMA Magazine: http://www.cgma.org/magazine/news/pages/201411089.aspx?TestCookiesEnabled=redirect

The Open Group. (n.d.). Cloud Computing for Business : Why Cloud? Retrieved February 2016, from The Open Group: http://www.opengroup.org/cloud/cloud/cloud_for_business/why.htm

Chia, T. (2012, August 20). Confidentiality, Integrity, Availability: The three components of the CIA Triad. Retrieved February 2016, from StackExchange: http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/

Henderson, J. (2015, July 31). Is cyber threat intelligence emerging as a “vital” security approach? Retrieved February 2016, from Computerworld: http://www.computerworld.co.nz/article/580876/cyber-threat-intelligence-emerging-vital-security-approach/

The Open Group. (n.d.). Cloud Computing for Business : What is Cloud? Retrieved February 2016, from The Open Group: http://www.opengroup.org/cloud/cloud/cloud_for_business/what.htm

EPIC. (n.d.). Veterans Affairs Data Theft. Retrieved February 2016, from Electronic Privacy Information Center: https://epic.org/privacy/vatheft/

PwC. (2014, December). Playing the part: Streamlining role-based access control. Retrieved February 2016, from PwC: https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/pwc-role-based-access-control.pdf

Published on: April 2016