Analysis, advanced key points of the article:

LOOKING AT CLOUDS FROM BOTH SIDES NOW

written by W. Kuan Hon, Christopher Millard & Ian Walden

SUMMARY

1. ANALYSIS HISTORY

- June 2014 : first revision
- January 2015 : second revision. No more security. Consequences on the market.

2. CONTEXT

Applications and Internet services have become necessary to the communication and the management of ongoing business activity.

Employees, managers and top executives use daily Internet applications and services.

Even though, the news regularly show how difficult it is for them to measure the risks on cloud computing offers for their company.

Since Edward Snowden disclosures, it is a known fact that :

- competitor companies can get access to confidential data through their states' eavesdropping,
- the NSA broke Internet infrastructure security to make this possible.

If you are a cloud service provider, you cannot longer guarantee the confidentiality, availability and integrity of your clients data.

When offering cloud computing services, it is important to analyze the related risks and reduce them.

We support you in this project.

3. THE EVOLUTION OF CLOUD COMPUTING ENVIRONMENT

3.1. The rise of Cloud Computing: from a marketing opportunity to a service

3.1.A. From providing of large scale hardware means to providing of large scale services

Having built complex infrastructures necessary to their operations, but needing competencies outside of their own core competencies group, companies feel the need to rationalize their risks through unloading these means to subcontractors.

After the development of large scale hardware means providing offers, it becomes possible to offer the providing of large scale services using these hardware means.

This way, the total cost of risk has been lowered by concentrating in the same place all the skills necessary to these hardware means and services management.

3.1.B. From a hardware means contract to a service contract

The contract is no longer about providing hardware resources, but about providing a service without even mentioning the underlying means.

The novelty in cloud computing is the assembling of contractual terms allowing to manage the commitments and risks implied by the service.

A company proposing a service which contract would only define the commitments without defining who is supporting the risks and what should be their management, is taking undefined risks possibly higher to those it can afford.

3.2. Only vertical integration players earn money

Cloud Computing providers invested thinking that by entering the market quickly and setting the service price, they would capture the market share and later recoup themselves by replacing the

hardware cheaply thanks to Moore's Law, which states that each two years, hardware price is halved.

Since Google has decided to reduce its Cloud Computing prices as the same rate as the hardware price reduction, this strategy has aborted and providers have exited the market the very same week.

Currently, only companies offering services based on cloud computing are making money, not those offering cloud computing services directly.

3.3. Edward Snowden disclosures consequences[1]

3.3.A. Before Prism, a safe ignorance

Before Prism, representatives of legal entities could legitimately use Microsoft, Yahoo, Google, Facebook, Paltalk, YouTube, AOL, Skype and Apple services without knowing that these companies were delivering information, some of it about confidential business, about their entities to third parties, including competitors indirectly.

Indeed, through the Prism program, the NSA has been spying trade secrets and sensitive information, that is to say, the added value and core assets of companies.

However, since the revelations about Prism, it is no longer possible to ignore that these nine services companies interfere in the private lives of citizens and businesses.

Individuals do commit only themselves. In contrast, representatives of legal entities represent their organization.

For the latters, using these services, and more generally services which data security procedures failures have been exposed, means to jeopardize the confidential data of their company.

3.3.B. Since Prism, voluntary ignorance is riskier than before

LOSS OF CONTRACTS

Since Prism, potential non-US Internet services customers are now reluctant to use Internet services U.S. companies.

1 Extract from Judith Lukoki analysis "Ignoring data security is taking part in an organized system of looting and plundering of data" http://blog.ethicalsocialnetwork.org/?p=1071

The loss for the cloud computing industry is valued at U.S. 180 billion over the next years.

To avoid a loss of customers, Google, the largest Internet company in the world (email, social networking, cloud, address book, calendar, etc.), offers from August 15th, 2013 to its business customers to encrypt their data for free.

This security measure is still inefficient as the data is encrypted with methods rendered ineffective by the very same NSA during their design and implementation. Still, it increases the cost to spy.

Destruction of telecommunications and Internet infrastructure security

> The NSA through its Prism programs and Aurora Gold[2] project destroyed for a long time the security of communications and Internet infrastructure.

Termination of contract

Customers may explicitly terminate their contract.

Potential customers may not enter into contracts with companies using the services and equipments of these nine companies, because it would jeopardize their business data.

> Up until now, the risk management work has been avoided, creating in itself a risk.
> Since Snowden disclosures, we know the event has been realized: our security tools were not in fact secure.
> It is now necessary to repair our operations to return to a standard level of exploitation.
> This implies to finally study and measure the risks related to the services contracts.

3.4. OpenSSL bugs: no more global security

A major bug has been discovered in OpenSSL, the software library used to encrypt most of the communications on the Internet.

This bug, called Heartbleed[3], is considered to affect most Internet services.

2 https://firstlook.org/theintercept/2014/12/04/nsa-auroragold-hack-cellphones/
3 http://heartbleed.com/

Some companies are managing this security breach as soon as possible: Apple did replace OpenSSL by its own proprietary code some years ago, and Google is currently replacing it while offering others the possibility to benefit from its own work on this[4].

Every company should now revise its security commitments and its risk policy to commit itself only in risks it is able to take on.

4 http://arstechnica.com/security/2014/06/google-unveils-independent-fork-of-openssl-called-boringssl/

4. CONSEQUENCES FOR SERVICE OFFERS

4.1. Unmeasured risk is too much risk[5]

A risk is an amount of money that you are going to spend for sure. When you do not calculate it, you just don't know how much and when you are going to spend this money, but still you are going to spend it.

A risk is the sum of probabilities, that is to say, the chances that an event takes place (natural disaster, reduction in the value of securities of a company, loss of contract, loss of profit, transportation accident, cyberattack, exposure of top executives professional emails, client information disclosure by an employee) multiplied by the cost of these events.

If the cost is sufficiently large, the risk may be higher than an event that happens often, but costs less. Insurance is a tool to reduce risk: if it costs less than the risk it covers, then it reduces the risk.

In the contractual relationship between some of the Internet service providers and their users/customers, the risk is asymmetric. The risk of the customer is to miss the guarantee of confidentiality or availability of their data or not to be able to verify its integrity.

The Internet services provider risks the loss of customers and loss of money through lawsuits for not being able to guarantee confidentiality or availability or integrity.

Whereas since the NSA disclosure, we all know this is something impossible to guarantee.

This is the case among cloud computing actors.

4.2. Deductibility of risks provisions

Having identified and measured the risks, it is then possible, advisable and in some cases mandatory to set aside provisions.

Those provisions are deductible from taxable income.

5 Extract from Judith Lukoki analysis "Security never goes without saying"

4.3. Adapting the service

Companies adapt in time their services, so their legal and business risks too.

The company must implement a legal and technological watch concerning its service (evolution of behaviors, scandals, technological breaches of security, Law and judges decisions).

4.4. Adapting continuously its obligation of means and obligation of result

In the current environment, companies offering cloud services must limit their risk for each core element of the contract.

For each of those, generally including confidentiality, availability and integrity, the company must decide which obligations of means or of result are relevant.

This implies to create the necessary tools to measure the respect of their obligations.

The availability is generally measured. However, the confidentiality and integrity are not.

Banks, telecommunication companies, big size companies do revise continuously their obligations due to the evolution of their services.

For the same reasons, companies offering cloud services must have adequate processes to adapt continuously their contracts.

It is imperative for those evolutions to be accepted to explain them in intelligible plain language.

> It is important to note that no company should currently offer data confidentiality in its cloud services, as it is now impossible to provide.
>
> In case of confidentiality breach, it would rightly be sued by its customers, and then have to take responsibility on the consequences, among them loss of activity damages, which may be greater than what the company is able to support.

5. THE KEY ISSUE OF SECURITY "COMMON SENSE"

5.1. The impact of security "common sense"

The common security concept is directly related to the local country risk culture.

Thus security expectations depend on the country.

For example, in France, it implies to "do your best" to ensure security. Because the society is built in a way everybody is responsible for everybody, french people generally voluntarily ignore some events called risks. When we do this, we do not calculate them. Citizens when acting as employee act in the same way. For a citizen this kind of risk management may work but it is not the case for a company.

In Germany, it implies to "do what you must". In this kind of society, citizens are incline to do every time what they must do. This kind of citizen risk management make people calculate their risk in their private life. They do the same in their professional life.

In the United States of America, it implies to communicate to the authorities the information they ask.

Chinese units of KPMG, Deloitte, PricewaterhouseCoopers, Ernst & Young refused to communicate to american authorities the audit work papers of certain Chinese companies under investigation for accounting fraud. The SEC judge suspended them from practicing for six month in the US[6].

5.2. Adapting the obligations of means and of result to local common sense

As security expectations depend on the country, cloud computing service providers have to explicitly adapt their commitments to this common sense, sometimes to several of them.

For example, if a company's client is present at the time in France and in the USA, then the company must explicitly, when defining its contract, take into account both common sense and eventually respect at the same time the european and US regulations while aiming at minimal risks.

Cloud service providers must thus measure the risks related to their services to operate, sometimes simultaneously, with different, sometimes contradictory, regulations.

6 http://www.cnbc.com/id/101356860

6. YOUR KEY CONTACT

Digital business risk consultant: Judith Lukoki

Phone number: +33 (0)6 15 94 50 23

E-Mail: judith@e-smconsulting.com