Cloud Service Providers – Protection of Critical Information Infrastructure

ATTILA HORVÁTH PHD
Senior Researcher – Fondation for Information Society
horvath.attila@infota.org

ABSTRACT

The prevention of data loss is one of the key buzzwords within the promotion activity of the cloud service providers (CSP). This article come round the main security issues of cloud services, which any decision maker have to take into consideration when choosing a CSP or specifying a private cloud service. The strengths and weaknesses of cloud architecture are examined closely from the security point of view to conclude in a system of aspects for decision makers to take into consideration before changing to cloud based services.

Introduction

The Infocommunication Technologies (ICT) is more and more affecting our lives. The application of these technology drivers covers both the homes and the economy. We take their presence as granted. They are parts of the everyday infrastructural services. Therefore their deficiency or absence can so severely affect the economic role-players or households as the missing of any other critical infrastructural resources.

Security issues, the importance of its proper configuration and operation is now an evidence for the business sector and the security-consciousness of the public and private sector is rising constantly as well.

The spreading of the new, cloud based services, the situation changed somewhat. Public clouds promise a new level of data security and accessibility to their users. The prevention of data loss is one of the key buzzwords within the promotion activity of the cloud service providers (CSP). The corporate and even the public sphere tends to think on moving to the cloud in order to enhance data security, service level, stability and cost-effectiveness of the services.

But who watches the watchers? Cloud service providers – although they really make reaching a higher level of services possible – are not identical, particularly from security point of view. To choose the proper service provider or to make a decision about starting a private cloud base service, a higher level of trust among the client and the service provider is needed, as by entering the cloud, it becomes virtually impossible to trace the real processing our data, clients, etc. are going through, only assumptions are at hand according to the specifications and service level agreements (SLAs) with the CSP.

The EU member states have committed to protecting critical ICT systems via the European Commission's CIIP (Critical Information Infrastructure Protection) [4] action plan by preventing large cyber-attacks and cyber disruptions of critical ICT systems. This article examines this approach, analyses the matching security governance, and particularly the proper risk assessment points of the topic.

This research is part of a larger research project concerning the effects of IT and network vulnerabilities on economy and society, which is implemented by the author in ligament with the Foundation for Information Society with the correspondence of the National Cybersecurity Center and the support of Hungarian Scientific Research Fund – project number: PD-109740.

A brief definition of cloud computing

Cloud computing is an on-demand service model for IT, often based on virtualization and distributed computing technologies. [4] Cloud computing architectures have:

- Highly abstracted resources
- Near instant scalability and flexibility
- Near instantaneous provisioning
- Shared resources (hardware, database, memory, etc)
- 'Service on demand', usually with a 'pay as you go' billing system
- Programmable management (e.g., through WS API).

There are three categories of cloud computing:

- Software as a service (SaaS): is software offered by a third party provider, available on demand, usually via the Internet configurable remotely. Examples include online word processing and spreadsheet tools, CRM services and web content delivery services (Salesforce CRM, Google Docs, etc).
- Platform as a service (PaaS): allows customers to develop new applications using APIs deployed and configurable remotely. The platforms offered include development tools, configuration management, and deployment platforms. Examples are Microsoft Azure, Force and Google App engine.
- Infrastructure as service (IaaS): provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API. Examples include Amazon EC2 and S3, Terremark Enterprise Cloud, Windows Live Skydrive and Rackspace Cloud.

Clouds may also be divided into:

- Public: available publicly - any organization may subscribe
- Private: services built according to cloud computing principles, but accessible only within a private network
- Partner or Community: cloud services offered by a provider to a limited and well-defined number of parties.

Uptake of Cloud Computing

Public and private sector organizations are switching to cloud computing: While years ago software applications were running on servers on their own premises or dedicated data centers, now applications are outsourced to large cloud service providers and run in very large data centers.

Cloud computing is being adopted rapidly across society, and across different sectors of society. Many analysts predict a further growth (of around 20-30% a year). Some examples:

IDC reports public IT cloud services will reach $47.4B in 2013 and is expected to be more than $107B in 2017. Over the 2013–2017 forecast period, public IT cloud services will have a compound annual growth rate (CAGR) of 23.5%, five times that of the IT industry as a whole. The growing focus on cloud services as a business innovation platform will help to drive spending on public IT cloud services to new levels

throughout the forecast period. By 2017, IDC expects public IT cloud services will drive 17% of IT product spending and nearly half of all growth across five technology categories: applications, system infrastructure software, platform as a service (PaaS), servers, and basic storage. Software as a service (SaaS) will remain the largest public IT cloud services category throughout the forecast, capturing 59.7% of revenues in 2017. The fastest growing categories will be PaaS and Infrastructure as a service (IaaS), with CAGRs of 29.7% and 27.2%, respectively. [6]

Gartner predicts that the bulk of new IT spending by 2016 will be for cloud computing platforms and applications with nearly half of large enterprises having cloud deployments by the end of 2017. The worldwide cloud-based security services market will be worth $2.1B in 2013, rising to $3.1B in 2015. [2] In the next five years enterprises will spend $921B on public cloud services, attaining a CAGR of 17% in the forecast period. [8]

McKinsey & Company projects that the total economic impact of cloud technology could be $1.7 trillion to $6.2 trillion annually in 2025. Of this total, $1.2 trillion to $5.5 trillion could be in the form of surplus from use of cloud-enabled Internet services, while $500 billion to $700 billion could come through productivity improvements for enterprise IT. [7]

Similar figures are reported for the healthcare and financial services sector.

The public data tells only part of the story - from public data it is difficult to understand how many end-users or organizations depend on a cloud computing provider, because cloud computing providers often offer services to other organizations, which in turn provide services to the (sometimes millions of) customers. For example, a SaaS cloud computing provider who uses the cloud (an IaaS cloud computing provider) for computing and storage resources. [1] This kind of reselling of IT resources makes it hard to estimate how many end-users depend on a single cloud provider and this makes it hard to estimate the full impact of an outage in society. For example Amazon AWS infrastructure only is reported to carry as much as 1% of the all internet consumer traffic in North America and on an average a third of all internet users visit an AWS powered site daily and there are CSPs, like Rackspace, Google or Microsoft with similarly convincing numbers. [8]

Security governance elements

Considering the future and more excessive use of CSPs the goal would be to keep the data stored in the cloud uncompromised, prevent data breaches and security incidents. Cloud security governance, similarly to other areas, can be subdivided in three key processes, shown in exhibit 1 below:

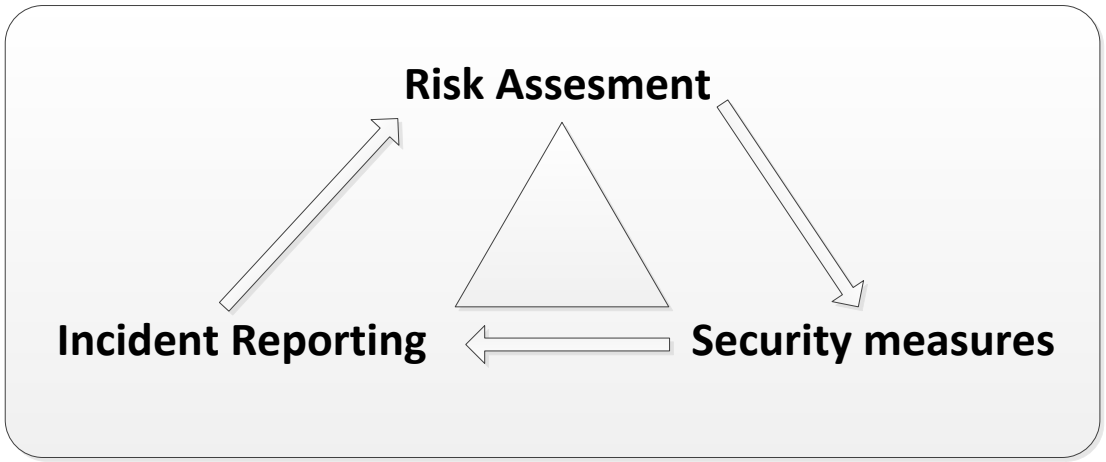

Exhibit 1.: The security governance cycle

Risk assessment

Many risks are related to certain business opportunities, made possible by the cloud architecture. Therefore it has to be taken into consideration whether these risks are compensated by the opportunities provided. The key is risk-consciousness.

Cloud services are not only about convenient storage, accessible by multiple devices, but include important benefits such as more convenient communication and instant multi-point collaboration. Therefore, the risks of using cloud computing should be compared to the risks of staying with traditional solutions, such as desktop-based models. The level of risk will in many cases vary significantly with the type of cloud architecture being considered.

It is possible for the cloud customer to transfer risk to the cloud provider and the risks should be considered against the cost benefit received from the services. However not all risks can be transferred: if a risk leads to the failure of a business, serious damage to reputation or legal implications, it is hard or impossible for any other party to compensate for this damage.

First of all it is needed to **define the most critical cloud computing services**. A widespread approach is that all cloud computing services are critical, but it is impossible to handle all cloud computing services at the same level. Since outages at IaaS or PaaS providers can have an impact across a range of organizations, this means that these services should be treated with priority. Often even SaaS-type services depend on an IaaS/PaaS-type services and all of them depend on network connection and power supply of course. So the most crucial part to sustain is the physical infrastructure, than IaaS/PaaS services and finally SaaS is the least critical, as it depends on all of the previous ones.

Most countries make national **risk assessments**, large companies also carry out such analyses. In these cases the critical infrastructure perspective is an important point of view. These assessments usually take into consideration only power supply and electronic communications networks, although they should also take into account large cloud computing services and large datacenters. [5] The modern society is highly dependent on IT.

A successful risk assessment requires **an honest identification of the true dependencies**. It needs to be clarified which critical operators and critical services depend on cloud services. The true nature of cloud services plays a two-faced role here. A baseline of cloud services that hardware and software is shared between multiple tenants. This makes it possible to withstand DDoS attacks or peak loads for example. At the same time, this benefit creates further cross-dependencies among the business and society. A fall out of a basic IaaS or PaaS provider can affect a wide range of (seemingly otherwise unrelated) services across everyday life. It is vital to map the main logical and physical dependencies.

Figure 2 below shows a roundup of the most common risk drivers of cloud technology. The risk drivers are evaluated according to two main dimensions: the probability of the event to happen, and the severity of the effects of the certain events. The risks are classified into three categories:

- Policy and Organizational
- Technical
- Legal.

The figure below clearly shows that all three represent themselves in the highest probability-severest impact (red) section, so it is not enough to focus on one or two groups in the first place. All risk types have to be handled with equal attention. It also has to be pointed out, that the most serious risk driver is not a technological, but an organizational issue and it is usually the very first aspect to take into consideration when deciding about getting involved in the cloud technology at all.

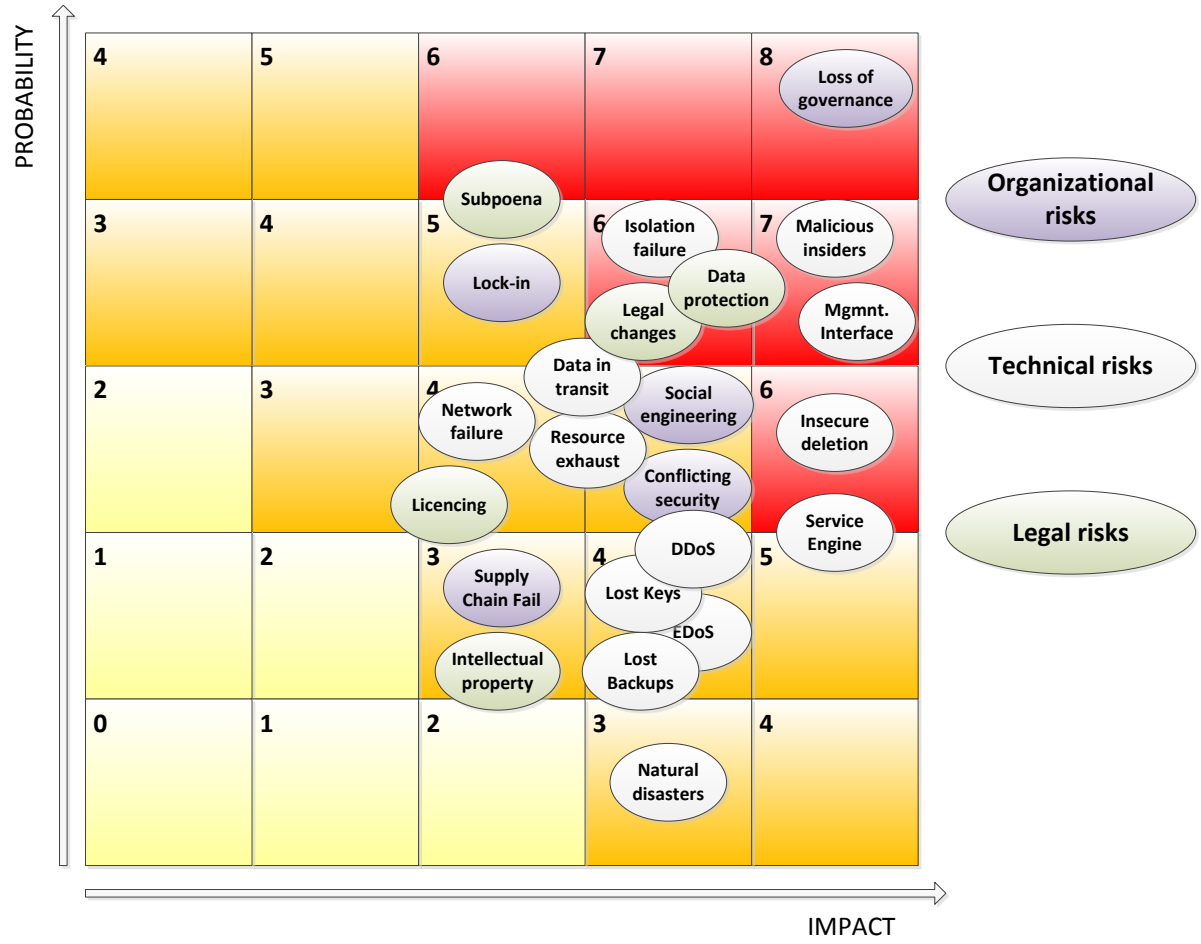

Figure 2.: Security risk distribution

If we look at the red-zone risk drivers, we find **an organizational risk – loss of governance** – at the top of the list, as mentioned above. In using cloud infrastructures, the client hands over control to the CSP on a number of issues which may affect security. Moreover, there may be conflict between the clients policy requiring the raising of security levels and the cloud environment, where security level is the liability of the CSP. On the other hand, SLAs may not offer a commitment to provide such services on the part of the CSP, leaving a gap in security defenses. Moreover the CP may outsource services to third-parties (unknown providers) which may not offer the same guarantees. In general, the lack of transparency can be a problem for the whole system. If a CSP does not declare which core IT services are outsourced - it is not realistic that providers should list the contractors since these may change frequently - the client is not in a position to properly evaluate the risk he is facing.

Further important risks are more **technology based** ones:

The **malicious activities of an insider** could potentially have an impact on: the confidentiality, integrity and availability of all kind of data, services, IPs and therefore indirectly on the organization's reputation, customer trust and the experiences of employees. This can be considered especially important in the case of cloud computing due to the fact that cloud architectures necessitate certain roles which are extremely high-risk. Examples of such roles include cloud system administrators and auditors.

The **customer management interfaces** of public cloud providers are Internet accessible and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk of being compromised especially when combined with remote access and web browser vulnerabilities.

This includes customer interfaces controlling a number of virtual machines and, most importantly, cloud providers' interfaces controlling the operation of the overall cloud system.

Multi-tenancy and shared resources are two of the defining characteristics of cloud computing environments. Computing capacity, storage, and network are shared between multiple users. **Isolating** the data and processes of the individual clients is a basic requirement awaited from every CSP. This class of risks includes the failure of mechanisms separating storage, memory, routing, and even reputation between different clients of the shared infrastructure (e.g., so-called guest-hopping attacks, SQL injection attacks exposing multiple customers' data stored in the same table, and side channel attacks). The probability is low in case of private clouds, but in case of public cloud environment it has to be seriously taken into consideration.

Data deletion problems are the last group of the high-risk technology based group. Whenever a provider is changed, resources are scaled down, physical hardware is reallocated, etc, data may be available beyond the lifetime specified in the security policy. Deleting data from Cloud storage does not in fact mean that the data is removed from the storage or eventual backup media. If disk storage is not encrypted, the data could be accessed at at later time by another customer of a Cloud provider.

There are some **legal issues** among the most severe risks as well.

Data protection is a key question, particularly under the strict European legislation. Processing data in another country may incur difficulties regarding the legal environment of data protection, or might even be considered unlawful by the responsible Data Protection authority. It can be difficult for the client (in its role of data controller) to effectively check the data processing that the CP carries out, and thus be sure that the data is handled in a lawful way. There may be data security breaches which are not notified to the controller by the CSP. Even the CSP may receive data that have not been lawfully collected by its customer (the controller).

The changes of legal environment also represent a severe risk for the clients keeping their data or services in a foreign and/or multinational CSP. There are numerous ways in which the change in jurisdiction could affect the security of the information.

Examples include:

- Data might be seized or the operations of a service disrupted due to reasons that do not even exist in the clients' country.
- In some cases, national security interests of the hosting country might be cited as a reason for seizing data.
- Additionally, a CP might be subject to law enforcement or national security actions from the country its business headquarters is based in, not just those from the countries where its data centers are located.

The list of points to consider just goes on and on. For length restrictions of this article the complete list of risk drivers will be accessible in the research study.

Security measures

It goes without saying that it is important that cloud providers take appropriate security measures. Security is constantly changing and security measures must be improved continuously. Authorities as well as corporate participants of the cloud industry should encourage an open culture of exchange experiences with proper security measures. Security is about continuous improvement and a situation where a specific set of best practices is cast in stone (by regulation or self-regulation) should be avoided at all costs.

Cloud computing services are often set-up with several redundant datacenters to withstand outages (due to power cuts or natural disasters, etc.). However, cyber-attacks usually capitalize and exploit software vulnerabilities, which are persist across the datacenters. These vulnerabilities can cause outages by themselves. Although cloud service providers have the means to prevent cyber-attacks in professional way it still is important to create also **logical redundancy** as part of the defense system – that is, to use different layers of defense and to use separate systems with a different logical structure, to cross-check transactions and to detect intrusions and attacks.

Standardization, especially for IaaS and PaaS services, would allow customers to move workload to other providers in case one provider has an issue. In case of a standardized service and necessary backups an outage can be survived more easily. In case of an administrative or legal dispute the backups can be simply taken to the site of another (competing) cloud computing provider. This kind of scenario is only possible when the cloud services infrastructure is standardized.

Security professionals always stress the importance of test and **independent audits**. This is not different in case of cloud services as well. Although it has to be pointed out, that ICT systems are constantly changing (software is updated daily) and that this reduces the significance of periodic (yearly) audits. Cloud providers and regulators should focus on a continuous program of audits, tests and exercises in place. Audits by external third parties are only one part of the bigger picture.

Incident reporting

To solve and learn from a security incident depends on whether the organization knows about it at all, or it remains the well-kept secret of the IT-security staff. Without incident reports it is very difficult to understand the impact of security incidents on cloud computing providers. Lack of data about incidents makes it very difficult to prioritize security measures, and in this way security governance becomes inefficient or even ineffective. There are many issues concerning this topic, but first it is very important to set the **reporting threshold** properly to provide adequate information for the management, the authorities, the regulators and the clients as well.

Certain cyber-attacks are very advanced and their trails may be difficult to scout even for security professionals who know the cloud computing systems inside out. For fear of sanctions, business interests or legal consequences there is a serious risk, that security incidents are **not reported** to higher management or to authorities. Providing **declared immunity** to colleagues and professionals working in the field of security.

While there is at least some information about data breaches, there are virtually no sources about cloud computing service outages. Even for the scares number of incidents came out into the open, it is difficult to find basic information like numbers of users affected or duration. To be able to assess the risks of clod technology and assess the effectiveness of cloud security, it would be crucial to have **public incident reports** about the cloud computing providers.

Conclusions

By examining the risk assessment approach to cloud computing the following conclusions are important to point out.

Cloud computing is critical: the usage is growing and in the near future the vast majority of organizations will rely on some form of cloud computing services. This makes cloud computing services critical in themselves. When cyber-attacks and/or disruptions happen, millions of users are affected. Cloud computing is present also in critical sectors, like finance, energy and transport.

Infrastructure and platform as a Service are the most critical branches of cloud computing.: Large IaaS and PaaS services which deliver services to other IT vendors who service in turn millions of users and organizations.

Cyber attacks which exploit software flaws can cause very large data breaches, affecting millions of users directly. The impact of cyber attacks is multiplied by the concentration of resources which is a result of the rapid implementation of cloud computing.

Elasticity is a key benefit of cloud computing and this elasticity helps to cope with load and mitigates the risk of overload or DDoS attacks. It is difficult to mitigate the impact of peak usage or a DDoS attack with limited computing resources.

A key benefit of cloud computing is resistance against regional power cuts or local natural disasters. It is difficult to mitigate the impact of fairly common regional disasters like floods, storms, or earthquakes in a set up with only a single datacenter, or a traditional set-up with a legacy onsite IT deployment.

Cloud computing is not immune to administrative or legal issues. If there is a legal dispute involving the provider or one of its customers, than this could have an impact on the data of all the other co- clients.

References

[1] Cisco: Cisco Global Cloud Index: Forecast and Methodology, 2012–2017, 2013. October, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf

[2] Columbus, Luis: Roundup of Cloud Computing Forecasts Update 2013, Forbes, 11.16.2013., http://www.forbes.com/sites/louiscolumbus/2013/11/16/roundup-of-cloud-computing-forecasts-update-2013/

[3] Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Critical Information Infrastructure Protection, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

[4] Dekker, Dr. M.A.C.: Critical Cloud Computing - A CIIP perspective on cloud computing services, European Network and Information Security Agency (ENISA) 2012. December, https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/critical-cloud-computing

[5] Dupré, Lionel – Haeberlen, Thomas: Cloud Computing - Benefits, risks and recommendations for information security, European Network and Information Security Agency (ENISA) 2012. December, https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security

[6] Gens, Frank: IDC Forecasts Worldwide Public IT Cloud Services Spending to Reach Nearly $108 Billion by 2017 as Focus Shifts from Savings to Innovation, IDC, 03.13.2013., http://www.idc.com/getdoc.jsp?containerId=prUS24298013

[7] Manyika, James et. al.: Disruptive technologies: Advances that will transform life, business, and the global economy, McKinsey Global Institute, 2013 May, http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technolgy%20and%20Innovation/Disruptive%20technologies/MGI_Disruptive_technologies_Full_report_May2013.ashxb v

[8] McMillan, Robert: Amazon's Secretive Cloud Carries 1 Percent of the Internet, Wired.com 18.04.2012., http://www.wired.com/wiredenterprise/2012/04/amazon-cloud/

[9] Shetty, Sony: Gartner Says Cloud Computing Will Become the Bulk of New IT Spend by 2016, Garner, 24.10.2013., http://www.gartner.com/newsroom/id/2613015