Published in International journal of information management, 2013, vol. 33, no. 5, p. 726-733
which should be cited to refer to this work

Risk perception and risk management in cloud computing: Results from a case study of Swiss companies

Nathalie Brender
Haute Ecole de Gestion de Genève
Campus de Battelle, Bâtiment F
7 route de Drize, 1227 Carouge, Switzerland
E-mail: nathalie.brender@hesge.ch

Iliya Markov
Haute Ecole de Gestion de Genève
Campus de Battelle, Bâtiment F
7 route de Drize, 1227 Carouge, Switzerland
Tel: +41 (0)22 388 17 27
Mobile: +41 (0)79 886 52 53
E-mail: iliya.d.markov@gmail.com
(corresponding author)

Abstract

In today's economic turmoil, the pay-per-use pricing model of cloud computing, its flexibility and scalability and the potential for better security and availability levels are alluring to both SMEs and large enterprises. However, cloud computing is fraught with security risks which need to be carefully evaluated before any engagement in this area. This article elaborates on the most important risks inherent to the cloud such as information security, regulatory compliance, data location, investigative support, provider lock-in and disaster recovery. We focus on risk and control analysis in relation to a sample of Swiss companies with regard to their prospective adoption of public cloud services. We observe a sufficient degree of risk awareness with a focus on those risks that are relevant to the IT function to be migrated to the cloud. Moreover, the recommendations as to the adoption of cloud services depend on the company's size with larger and more technologically advanced companies being better prepared for the cloud. As an exploratory first step, the results of this study would allow us to design and implement broader research into cloud computing risk management in Switzerland.

Keywords: Cloud computing; Risk management; Empirical results; Small and medium enterprises (SMEs); Swiss-based enterprises

1. Introduction

Cloud computing has grown enormously in recent years. In today's economic turmoil, the cost efficiencies of its pay-per-use pricing model offer an attractive alternative to in-house IT infrastructure. On an operational level, it increases the potential for innovation by freeing up resources and refocusing them on core business activities. Moreover, in an era of ubiquitous broadband, cloud computing responds to the needs of the mobile workforce of today by bringing collaboration to a whole new dimension. A recent report by Gartner research predicts that the global cloud market is expected to explode in the years to come (Gartner, 2012).

Cloud computing is nevertheless fraught with risks. Security, confidentiality, auditability, regulatory compliance and a host of other risks should be carefully examined before any engagement in this area. As Heiser and Nicolett (2008) of Gartner point out, by its very nature, cloud computing is the least transparent externally provided service method "storing and processing your data externally in multiple unspecified locations, often sourced from other, unnamed providers, and containing data from multiple customers." In consequence, they advise that organizations considering the adoption of cloud services must clearly understand the risks and define the necessary controls before any sensitive information is migrated to the cloud.

The main contribution of the present research is an empirical study of the risk and control analysis in relation to the prospective adoption of public cloud services by a sample of Swiss companies. The participants in the study are professionals who attended a course in Business Risk Management (Gestion des Risques d'Entreprise) at the Geneva School of Business Administration (Haute Ecole de Gestion de Genève). They worked in groups and submitted five reports each dealing with a specific company. The purpose of this study is to establish whether cloud computing risks are well understood and whether proper mitigation practices have been studied and proposed.

In short, we find a sufficient degree of risk awareness and the ability to focus specifically on those risks and controls that are relevant to the particular IT function to be migrated to the cloud. The recommendations of whether to adopt cloud services depend on the company's size, technological expertise, and corporate culture but not on the type of process or data to be migrated. To our knowledge, this is the first study of this kind to be conducted in Switzerland. Nevertheless, the inferences we make should be viewed in light of the small sample size (only five reports) and underline the need for broader and more detailed studies in the future.

This article is organized as follows. Section 2 is a definition of cloud computing and a description of some of its most important characteristics. Section 3 presents an overview of academic and technical literature on the general risks associated with it. Section 4 describes our empirical sample and extracts additional risks analyzed in the reports. Section 5 reviews several issues based on the reports' contents. Finally, Section 6 offers some concluding remarks.

2. What is cloud computing

The US National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011). According to NIST, the cloud computing model comprises five essential characteristics, three service models and four deployment models (Mell & Grance, 2011).

The characteristics are described as on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service (Mell & Grance, 2011). On-demand self-service denotes the unilateral provisioning of resources without human interaction with the provider while broad network access means that services are delivered over a network. Resource pooling is the aggregation of resources such as storage, processing, memory, bandwidth, etc. to serve multiple customers. Rapid elasticity indicates that resources are

dynamically scaled up and down with demand and, finally, measured service refers to the automatic control and optimization of resources through pay-per-use metering capabilities.

The three service models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) (Mell & Grance, 2011). IaaS denotes resources, such as processing, storage, networks, and other fundamentals, on which the customer can deploy operating systems and applications. Examples of such cloud solutions include Amazon's Elastic Compute Cloud (EC2), GoGrid's Cloud Servers, and Joyent (Sultan, 2011). PaaS builds on top of IaaS and offers an operating platform enabling the deployment of customer-created or existing applications that use the programming tools and libraries of the provider. Products in this category include Google App Engine, Microsoft Azure, Amazon Web Services (AWS) and Force.com (by Salesforce.com) (Sultan, 2011).

SaaS builds on top of IaaS and PaaS and provides a range of applications, such as word processing, spreadsheets, customer relationship management (CRM), HR management, enterprise resource planning (ERP) systems, etc., running on cloud infrastructure. SaaS has the lowest degree of customization with only limited control over some of the applications' configuration settings for off-shelf solutions such as Yahoo! Mail, Google Apps, Salesforce.com, WebEx, and Microsoft Office Live (Sultan, 2011). But users can also customize the products by developing specific components based on Application Program Interfaces (APIs) made available by cloud providers (Sultan, 2010). As a rule of thumb, the Cloud Security Alliance (CSA) (2011) explains that "the lower down the stack [IaaS, PaaS, SaaS] the cloud service provider stops, the more security capabilities and management consumers are responsible for implementing and managing themselves." In other words, in an IaaS architecture, the consumer is responsible for the security of the software deployed on it. At the other end of the spectrum, in a SaaS solution, the provider ensures the security of the applications they offer.

In terms of deployment, NIST distinguishes between private clouds, public clouds, community clouds and hybrid clouds (Mell & Grance, 2011). In private clouds, the cloud infrastructure is provided only for the use of a single organization. Private clouds give organizations more control over security, transparency and compliance but require substantial capital and operational expenditures and a highly proficient IT team (Carroll, van der Merwe, & Kotzé, 2011). Public clouds in turn provide cloud services for use by the general public.

Community clouds provide cloud infrastructure to several organizations sharing the same mission, security concerns, compliance requirements, etc. They have the advantage of cost efficiency compared to private clouds and reduced risks compared to public clouds (Carroll et al., 2011). Hybrid clouds are combinations of several cloud infrastructures (public, private or community) which remain separate but share common standards that enable data and application portability.

3. Cloud computing risks

As Hawser (2009) notes, cloud computing provides small and medium enterprises (SMEs) with access to software, services and infrastructure normally beyond their reach. In a survey of more than 70 SMEs conducted by the European Network and Information Security Agency (ENISA), 68.1% point to avoiding capital expenditures on hardware, software, IT support and information security as a reason for possible adoption of cloud services (European Network and Information Security Agency [ENISA], 2009a). OneStopClick's (2011) December 2010

survey of more than 3200 SMEs from 16 countries reveals that 40% plan to purchase cloud services in the next three years.

Cloud computing, however, presents significant risks and challenges as well. In a survey of nearly 1800 US businesses and IT professionals by the Information Systems Audit and Control Association (2010), 45% consider the risks of cloud computing as outweighing the benefits. The sections below review the main topics of concern with an emphasis on their interpretation from a management point of view. They are not ordered by severity but rather represent specialists' views regarding the major risks of cloud computing and the relevant mitigation practices.

3.1. Information security

As with any modern technology, information security remains a major concern in the adoption of cloud services. It is rated as the top threat in interviews with South African participants performed by Carroll et al. (2011). ENISA (2009a), in turn, finds that 43 out of 64 SMEs surveyed point to confidentiality of corporate data as a showstopper, with privacy mentioned by nearly a half. Sultan (2011) moreover cites a survey of chief information officers carried out by the International Data Corporation (IDC) with almost 75% of respondents saying they were concerned about security.

On the one hand, the technology's presence on the web and the massive concentration of data present a more attractive target for hackers (ENISA, 2009b). As Kaufman (2009) explains, providers like Amazon and Microsoft, for example, have the capabilities to deflect and survive cyber-attacks that not all providers have. On the other hand, cloud defenses rely on economies of scale and hence cost efficiency and on concentration of expertise in the provider. Moreover, the distributed nature of the cloud with data stored in multiple data centers limits damage due to such attacks (Biswas, 2011a). Therefore it is not necessarily a disadvantage for companies to perform activities on the web. As Biswas (2011a) stresses, an in-house IT department is not necessarily more secure than a cloud-based offering as it is still connected to the internet and thus susceptible to hacking attacks. Nevertheless, customers should ensure before signing up for a service that the security that the provider offers meets their requirements (OneStopClick, 2011). This issue is further heightened in the case where a cloud offering involves several different providers (i.e. a cloud provider outsourcing activities to another provider without necessarily informing the client) with the resulting product being as strong as its least secure provider.

3.2. Privileged user access

As Heiser and Nicolett (2008) point out, the processing of sensitive data outside the premises of an enterprise bypasses the "physical, logical and personnel controls" that an in-house IT department exerts. The concept of the cloud may therefore become misleading as customers forget that their data is ultimately stored somewhere in a physical environment (Popovic & Hocenski, 2010). This brings us to the risk of a malicious insider who may cause brand damage, and financial and productivity losses to the customer (Cloud Security Alliance [CSA], 2010). Customers are therefore advised to require information on the hiring and oversight of privileged cloud administrators (Heiser & Nicolett, 2008).

CSA (2010) reviews some of the top threats in this category, namely account and credentials hijacking. If an attacker manages to steal a customer's credentials they will be able to access their cloud services, track their activities, manipulate their data, and redirect visitors to

illegitimate websites, which could lead to damage to reputation and financial loss, and be the base for subsequent attacks. The remediation solutions revolve mainly around policy, such as a strong authentication process, no shared accounts, and a proper understanding of the service level agreements (SLA).

Experts advise on the use of the least privilege principle (CSA, 2011; ENISA, 2009b). “This principle maintains that an individual, process, or other type of entity should be given the minimum privileges and resources for the minimum period of time required to complete a task” (CSA, 2011). Moreover, the same person should not have access to more than one related function (CSA, 2011). This opens the question of how the accounts with the highest level of privilege are authenticated and managed (ENISA, 2009b).

3.3. Regulatory compliance and data location

CSA (2011) explains that the European Economic Area (EEA) has enacted data protection laws[1] requiring that the obligation to provide adequate data security should be passed down to subcontractors. Similar laws have also been passed in many other countries as well. In general, they establish that the custodian is ultimately responsible for ensuring the protection, security and integrity of the data regardless of location, and especially when they are passed to a third party. The custodian remains liable for any loss, damage or misuse of the data.

Heiser and Nicolett (2008) note that traditional cloud providers submit to external audit and security certifications and provide customers with information about the security controls that have been evaluated. They advise that any provider that is unable or unwilling to undergo such audit or reveal the audit findings should only be considered for the most trivial functions.

Related is the issue of data location in public clouds. This is a big concern especially with regards to the privacy regulations in different jurisdictions (Heiser & Nicolett, 2008) or when the data reside in high-risk countries where governments may pass legislation that grants them access to all data within their borders (Biswas, 2011b). The Canadian government, for example, has noted that data held in US-based data centers may be accessed by the US government as provided for by the Patriot Act (Treasury Board of Canada Secretariat, 2010; Biswas, 2011b).

In addition, as CSA (2011) points out, many governments prohibit or restrict the transfer of data outside the country. They may only allow it if the host country offers adequate protection of personal information and privacy rights. Sultan (2011) adds that the EU governments have privacy regulations that prohibit the release of certain data outside of the EU. In response, companies like Microsoft and Amazon allow the customer to choose the physical location of the data, for example EU.

In Switzerland, Art. 6 of the Federal Act on Data Protection states that “personal data may not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection.” With regards to banks, the Swiss Financial Market Supervisory Authority’s (FINMA) Circular 2008/7 provides strict rules in relation to the outsourcing of banking activities. The Federal Act on Data Protection is under revision and the changes are expected to take effect in 2014.

[1] In the EEA, data protection laws derive from the 1995 European Union Data Protection Directive and the 2002 ePrivacy Directive (as amended in 2009) (CSA, 2011).

As a result, Circular 2008/7 will become stricter with regard to the outsourcing of banking data.

3.4. Investigative support

As Cunningham (2009) notes, the pre-trial collection of electronic evidence in a lawsuit, known as e-discovery, assumes that an enterprise knows exactly where the data are located and how they are backed up and secured. It also assumes that the enterprise has the ability to physically examine storage media for deleted files, for example. When the enterprise stores its data on the cloud, it has little to no visibility to the storage and backup processes of the provider or the physical storage media themselves.

Heiser and Nicolett (2008) add that a single storage device may contain data and logging from multiple customers which poses challenges to understanding the access and deletion of files, and further from a privacy point of view. The data may also be located in different, often changing, data centers. Moreover, conducting forensic investigation even on an enterprise's own infrastructure is difficult, time-consuming and expensive.

If the enterprise relies on cloud services for the processing of business records or anticipates the need for investigation it has to factor in the inability or unwillingness of the provider to support it (Heiser & Nicolett, 2008). If the customer is unable to obtain a contractual agreement for the support of certain investigation activities and evidence that such were supported in the past, then they will probably not be supported in the future (Heiser & Nicolett, 2008).

3.5. Availability and disaster recovery

Availability of cloud services, especially for critical business processes is essential. If you are an online retailer whose retail platform is on a cloud, its failure can have serious repercussions to your business (Prakash, 2011). Heiser and Nicolett (2008) advise that any enterprise wishing to outsource critical business processes to the cloud should define, together with the provider, an SLA for the availability of service for critical business processes.

As Sultan (2011) points out, Salesforce.com was unavailable for 6 h in February 2008, followed by Amazon's S3 and EC2 clouds only several days later. Amazon's S3 was unavailable again for 8 h later that year. The list of similar accidents extends to more recent years as well with the multi-day failure of Amazon's EC2 in April 2011. As ENISA's (2009a) survey shows, 28 out of 66 SMEs consider availability of service and data as an issue of critical importance. On the other hand, the availability of service in many cases, and in particular with respect to SMEs, surpasses the availability that an in-house IT department can maintain.

Closely related is the issue of disaster recovery. In the interviews of Carroll et al. (2011), it receives 66.7% of the votes as an area of critical importance and ranks second after information security. From another prospective, ENISA (2009a) finds that 52.8% of SMEs cite business continuity and disaster recovery capabilities as a driver for possible engagement in cloud computing. It is therefore important for businesses to require information on what happens to their data in case of disaster and how long the recovery process lasts (Prakash, 2011).

3.6. Provider lock-in and long-term viability

As Sultan (2011) explains, many cloud providers use proprietary formats for application programming interfaces (APIs), data import and export, the storage of server images for disaster recovery, etc. As the number of providers grows, the portability and interoperability concerns will become even greater. Such concerns are further exacerbated by possible provider failures. Related, therefore, is the issue of long-term viability considering the implications of potential bankruptcy of the provider or its acquisition by another company. (Heiser & Nicolett, 2008). Customers should ensure that the SLA covers such scenarios and that their data will be available and they will have the ability to transfer it to a replacement application or another cloud provider (Heiser & Nicolett, 2008).

Scheier (2009) gives several examples of failures such as those of web application development provider Coghead and online storage facilities The Linkup and Upline. Even though Coghead's intellectual property was purchased by enterprise software developer SAP, Coghead's customers were given less than three months to retrieve all their data and applications.

Scheier (2009) proposes several steps to mitigate the effect of provider failure. He suggests that customers should inspect providers by performing checks on their revenues, profitability, number of customers, etc. as they would with any other vendor. They should also regularly back up their data and applications on local servers which requires maintaining local storage capacity and leads to the issue of application and data portability again. Customers should have contingency plans for data and application porting and enquire whether the provider offers technical support in such scenarios.

4. Cloud computing in a Swiss context

One of the few studies of Swiss businesses' engagement in cloud computing was conducted by consulting firm Cambridge Technology Partners (Zekrya, 2011) and includes mostly large enterprises open to new technologies. It reveals that cloud computing is successfully implemented in Switzerland with the preferred model being IaaS deployed on a private cloud. The study reports that the main advantages of cloud computing are flexibility and immediate access. In 83% of the companies, it also led to a reduction of the size of their IT departments. Interestingly, for 46% of the companies, corporate culture is the main obstacle to the adoption of cloud services. Security, reliability and confidentiality also remain important issues while price and migration problems cause less concern.

We contribute to the burgeoning research on cloud computing with a study based on the work of 19 participants enrolled in Business Risk Management (Gestion des Risques d'Entreprise), a continuing education program offered by the Geneva School of Business Administration (Haute Ecole de Gestion de Genève). They worked in groups and submitted a total of five reports analyzing the risks and challenges and proposing mitigation practices in the adoption of public cloud services by five companies based in Switzerland. Each report is focused on a single company and deals with the externalization of a specific IT function – or more - to a public cloud. As part of each company's approach to cloud computing, their analysis is mainly based on observation, study of documentation, group discussions or interviews with key stakeholders (company's managers, cloud providers, external experts). The IT functions in question, short descriptions of the companies and risk analysis summaries are given below:

- R&D: A biopharmaceutical company whose R&D software allows employees to track, edit and share sensitive information during all stages of the drug development process. In order to support its R&D activities that can be demanding in terms of computing power and involve a large number of stakeholders worldwide, the company is looking to select a cloud based provider to support its homemade solution. As part of an initial risk analysis, the following elements have been identified: legal risk as the solution is subject to national pharmaceutical regulators; intellectual property as the value of the information contained in the software represents years of research and significant budgets, security and confidentiality, lack of control and governance due to the outsourcing of a key company process, and finally, a cost increase. The risk management function considers that the risks can be mitigated but still recommends to contract with a specialized consulting company to accompany the firm in its approach to cloud computing and to maximize its success factors.

- Book exchange platform: An e-commerce company whose book exchange platform is connected to an accounting software. The platform enables students to exchange or sell/buy academic books. It could be compared to a specialized eBay and presents similarities in terms of users' ranking or payment mechanisms. The company's turnover is made of commissions collected on each transaction. To extend its customer base and strengthen its customer retention, the company is looking for the implementation of a cloud-based Customer Relationship Management (CRM) solution. The company is also envisioning an overall transfer of its platform to a public cloud solution in order to more easily absorb peaks of activities that occur at the beginning of each academic semester. The risk analysis highlights twelve risks: unavailability of the solution, performance risk, denial of services, overall governance and compliance of the solution, data protection, data backup, transaction security, legal risk, supplier dependency and lock-in, reputation, return on investment (ROI) and supplier selection. While compensation measures such as SLAs or the contract's evolution have been identified and deemed acceptable to mitigate identified risks, the management concludes that a cloud-based approach should be pursued with PaaS and not Saas. Its first argument highlights the integration of the overall approach in the IT governance and the limited capacity of the company to develop a suitable SLA due to its small size. The second argument is linked to the complexity of the provider selection process and the capability of the company to assess the provider's long term viability.

- ERP: A construction company whose inventory management system allows it to monitor, order, replenish and optimize its inventory stock and manage suppliers and billing. The company is looking to deploy the software in order to optimize associated costs. The foreseen solution should be able to handle three key processes: inventory management, supplier management and construction sites. The company carried out an analysis to implement a public cloud based solution that led to the identification of six major risks: exclusive dependency toward a supplier, supplier's potential bankruptcy, inter-cloud tenancy information leakage, data leakage, data persistence after contract's termination, and network failure. For each of the identified risks, mitigation scenarios have been developed and a cost/benefit analysis performed. However, the risk management function concludes that the company's maturity is not

sufficient to carry out such a project and will reassess the situation eighteen months later.

- Online training platform: An international oral medicine company wishing to create an online information and training platform to reduce the cost of on-site training. As a state-of-the-art eLearning solution is complex to develop and could require important infrastructure (i.e. for video streaming), the company is envisaging to adopt a cloud-based solution. An internal analysis identified the following major risks: IT governance risk, loss of control over IT infrastructure, system availability, intellectual property protection, content integrity, data leakage, dependency toward one provider, legal exposure and compliance. An appropriate governance and a formalization of a clear SLA with the solution provider should ensure the risk mitigation and constitute the basis for the deployment of the cloud-based solution.

- Trading room: A private bank providing financial services and asset management to high-net-worth individuals. The bank's trading room allows it to manage a multi-billion franc portfolio. This trading room is directly connected to key markets and stock exchanges. In order to optimize its cost structure, the bank is looking to outsource the totality of the IT infrastructure supporting the trading room. Due to the limitations imposed by the regulatory framework, the bank has identified a limited number of suppliers that could meet all the requirements and conducted an extensive risk analysis. The following risks were identified: ISO functionality; efficiency/speed – the functioning of the trading room is time critical, confidentiality, integrity, availability and compliance. While the analysis leads to the conclusion that most of the identified risks could mitigated or accepted, the ROI analysis shows that adopting the cloud solution would not be cost-effective. This is the only report evaluating the services of a specific provider the choice of which is based on its financial strength, responsiveness, the ability to provide reasonable assurances regarding availability, continuity and security, and, above all, the fact that its data centers are based in Switzerland.

The companies in question are anonymized for confidentiality reasons. Nevertheless, based on the available information we can extrapolate that the first two companies in the above list can be classified as SMEs and the rest as economically significant enterprises[2].

The reports to various degrees cover all the essential general risks outlined in Section 3. They also mention more specific or technical risks indicating awareness of a wide variety of potential threats in migrating to a cloud service. The reports converge on the need for careful negotiation and definition of the SLAs. As one report mentions, however, the position of each party to negotiate the SLA clauses depends on its size. Even if there is no explicit opportunity for negotiation, providers wishing to attract major players will strive to meet their regulatory and compliance expectations. However, while companies express their need for customized cloud solutions, in particular in the financial sector, cloud providers still tend to offer standardized SLAs.

[2] According to Swiss law and applicable from 1 January 2012, an economically significant enterprise is one in which at least two of the following figures are exceeded within two consecutive financial years: (1) balance sheet total of CHF 20 million, (2) revenues of CHF 40 million, (3) annual average of 250 full-time employment positions

The risks considered in the reports can broadly be classified into political/legal, operational and technical. Risk terminology, the number of risks and the perception of their severity, however, are not homogeneous across the reports. The risks below are those mentioned in the reports in addition to the ones in Section 3 or going into more details and are not ordered by severity.

4.1. Teething problems

The migration to a cloud service means that a company's employees and/or clients may have problems understanding how the new technology works. To mitigate this problem, the company could, in an initial stage, migrate only part of the IT function to the cloud. After testing and successful evaluation, the second phase will involve full externalization. The migration of data and applications may also face compatibility problems. Such can be overcome with the assistance of developers which will nevertheless lead to higher costs. Moreover preventative measures to avoid data loss during the migration stage should be put in place.

4.2. Application performance on the cloud

The performance of the migrated IT function depends on the quality of the solution offered by the cloud. One of the reports (book exchange platform) notes that users leave a website after 10 s or cancel a financial transaction if response time is not satisfactory. Such a risk can be considered critical as it can impact direct sales, lead to loss of customers or inability to attract new customers. One of the solutions proposed here again involves an initial testing stage to assess performance. Another measure is to optimize the interface between the cloud and the existing in-house technology by simplifying coding. The customer should also ensure that the SLA guarantees a minimum level of performance through clear and precise reporting metrics.

4.3. Loss of governance

A major risk in cloud computing is the loss of governance over the IT infrastructure. In addition to security and confidentiality issues, this could raise problems pertaining to regulatory compliance and auditability. As the enterprise has no control over the outsourced services it may, in extreme cases, be faced with the risk of reputation damage, prosecution, fines, etc. The cloud provider should therefore ensure that all the information about the financial accounts remain auditable by external auditors. All documents should be properly secured and maintained and be available to the customer at all times. This risk is considered strategic. Defining common frameworks for certification such as COBIT or ISO is suggested.

4.4. Determination of the competent authorities in case of conflict

As is often the case, the cloud provider and the customer may reside in different jurisdictions. They can therefore decide on the competent court in case of conflict. There is no absolute answer as to whether it is better for a Swiss company to choose a Swiss court or a court in the provider's jurisdiction. Choosing a Swiss court has the advantage of familiarity with the relevant legislation and ease of compliance. However, there is uncertainty as to the applicability of its decisions in the provider's jurisdiction. Choosing a court in the provider's jurisdiction on the other hand has the advantage of ease of application of the court's decisions but is contingent on the laws of that jurisdiction and the complexity of the legal

procedures. Swiss customers are therefore advised to choose a Swiss or an EU provider which will ensure adequate data protection and reduce uncertainties.

4.5. Cost

Some of the reports view the cost of moving to the cloud as a risk. As one report (R&D) notes, the cost of cloud services is clearly advantageous but it is important to beware of future costs due to the complication of the system or the inability of IT staff to manage the links between the in-house applications and those deployed on the cloud. It recommends the use of a consultant through the initial deployment phase until the company has complete control over the applications and infrastructure used. Another report (trading room) explains that the agreed level of service should be defined in detail in order to minimize the leeway for interpretation and should account for the needs of the data and applications to be migrated. Any changes to the company's needs potentially induce a deviation from the SLA in terms of capacity provision and will necessitate a renegotiation of the terms.

4.6. Economic denial of service

Pricing for cloud services is normally on a pay-per-use basis. An economic denial of service (EDoS) attack consumes the resources of the victim and increases their bill by generating a large number of transactions. The consequences of such attacks are twofold – they impact the availability of service and may cause an explosion of costs. As some of the cloud customers are more susceptible to such attacks they may spread the threat to other co-tenants as well. This risk is therefore considered critical. The SLA should specify that the provider cannot include the cost of such attacks in the bill and should be able to prevent them and offset their potential effects.

4.7. Data segregation

In the multi-tenant structure of cloud computing, data from different customers are in a shared environment. Poor segregation of resources therefore increases the risk of a security breach from a co-tenant due to lack of proper sealing. Such an attack may be carried out by a malicious co-tenant or by an outside attacker through a less secured co-tenant. Several reports note that this risk can be overcome by ensuring complete isolation of customer data on a dedicated physical server. According to an evaluation in one of the reports (R&D), however, a dedicated physical server can be twice as expensive as a virtual server.

4.8. Data destruction

When the customer decides to destroy particular data the provider must be able to guarantee its actual destruction. In fact, the data may be available well after the lifetime specified in the security policy of the provider. As far as the actual and total destruction of data is concerned, it is only possible after physical destruction of the storage media[3]. A measure to reduce this risk is to ensure that all data are encrypted, pseudomized or anonymized. Another measure is to ensure with a legal contract (with certification or audit requirements) that the provider should destroy all data or face the risk of financial or criminal penalties.

[3] Other methods such as storage media overwriting and degaussing also exists. The 100% effectiveness of overwriting however is contended and degaussing may render storage media unrecoverable.

4.9. Data traceability and monitoring of irregular activities

When migrating data to the cloud it is available in electronic format that can easily be downloaded on a USB stick or sent via emails. In order to ensure complete traceability of all data inventory, one report (ERP) proposes a watermarking solution. This technique allows information related to access and use to be added to any digital file. Closely linked is the issue of monitoring of irregular activities. When users access the cloud service, they normally use it with stops (i.e. short sequences). A long and uninterrupted use of the service may signal data collection or archiving for the purpose of exporting. The provider should have the controls in place to detect such behavior.

4.10. Security during data transportation

Data must be protected not only at rest but also during transit. Lack of adequate protection during data transfer may lead to attacks such as sniffing (listening to network traffic) and spoofing (assuming a sender's identity). The best protection against such attacks is data encryption although one report also suggests anonymization (trading platform). The customer must also ensure that there is no major disparity between their own security practices and those of the provider as such may lead to security gaps and penetrability of the system. Another mitigation practice proposed by two reports (R&D and trading room) is the use of a dedicated secure line between the provider and the customer.

4.11. Security of financial transactions

If the exchange of information between individuals and financial institutions is not sufficiently secure this may lead to data leakage. This risk is regarded as critical as disclosure of personal financial information may have legal consequences and bring reputation damage. Cloud customers must ensure that the security policies of the provider in dealing with financial data are in line with their expectations and requirements. The SLA should denote the provider's use of a secure Internet protocol for financial transactions.

4.12. Physical security and natural disasters

The risk that a provider may suffer from a physical intrusion is high due to the centralization of resources. Although the probability of such attacks is low as physical resources are generally well protected, their impact can be serious. The authors of one report (trading room) state that they have made physical inspection of the provider's site to assess the security of the systems and buildings. Closely linked is the problem of natural disasters which can severely affect a data center due to weak or untested resilience plans. One report (ERP) suggests a transfer of such risks with the customer taking insurance against the potential decline of service.

5. Discussion

After considering the risks and mitigation practices, four of the reports issue recommendations as to whether the respective IT function should be migrated to the cloud. Two reports conclude that the risks are manageable and favor the migration (trading room, online training platform), one favors the adoption of a PaaS as opposed to SaaS service model as the former gives more control over security (book exchange platform) and one suggests that the cloud solution is not secure enough and the company is not ready to adapt

(ERP). One report does not issue a specific recommendation but gives the impression that appropriate mitigation practices should reduce the risks to a manageable level (R&D).

The small sample of reports does not allow us to explicitly test whether their contents relate to the company size or the data or process to be migrated to the cloud. Nevertheless, we review the following issues based on a qualitative analysis of the reports.

The reports deal with the externalization of IT functions of various types. The report on the externalization of the book exchange platform, for example, treats the problem of the security of financial transactions as users pay for the services with credit or debit cards. It also treats the problem of the speed and performance of the cloud solution as customers are dissatisfied if response time is slow. The latter is also discussed in the report on the externalization of the trading room where performance is critical. Similarly, the reports on the R&D software and the online training platform refer to the protection of intellectual property. The reports therefore do not just blindly review the risks and prescriptions but are able to extract or suggest those that best suit the company's situation.

The migration of critical business processes to the cloud involves risks such as inadequate performance, lack of availability and loss of governance. In addition, the migration of sensitive data involves security, confidentiality, privacy and regulatory compliance risks as outlined in the previous two sections. However, the process criticality and data sensitivity do not appear systematically as the main criteria for the decision to adopt cloud solutions. On one hand, the report on the externalization of the trading room, a critical business process, concludes that the services offered by the provider are adequate for the purpose. The report on the externalization of inventory management, on the other hand, recommends that the adoption of cloud services should be postponed.

The final recommendation of whether to adopt cloud services seems to be related to the company's size. Size dependence, however, has more than one dimension. On the one hand, cloud services are attractive for SMEs as they would allow them to avoid investing in IT infrastructure and to use software they would normally be unable to afford otherwise. In contrast, larger companies have more financial and physical resources to maintain in-house infrastructure which would give them better control over the security and confidentiality of their data and the performance of their critical business processes. On the other hand, larger companies rely on more advanced risk management and more proficient IT teams when it comes to cloud related risks. Larger companies also possess broader technological expertise which makes them better prepared to embrace new technologies. The reports also suggest that larger companies (online training platform, trading room) are better prepared for the cloud. The construction company (ERP) report, however, does not recommend the adoption of cloud services. Even though it is economically significant, the report makes it clear that the company is not technologically advanced. As far as smaller companies are concerned, the R&D report does not issue a specific recommendation, while the book exchange report recommends a PaaS solution as opposed to SaaS.

Another explanation may be attributed to the corporate culture of some of the enterprises as noted by Zekrya (2011). Confidentiality and precaution that characterize Swiss business culture may constitute an internal barrier to the adoption of cloud computing solutions. Culture structures the mind-set of individuals and social organizations to adopt certain values and reject others; and these values determine the perception of risks and benefits (Douglas and Wildavsky, 1983). This may help to understand the contradictions between technical risk analyses and decisions made by management, as the construction report (ERP) suggests it.

In addition, perceived risks appear to be related to customers' insecurity about the control of a process and the lack of tangible elements to evaluate the complex service provided (Heskett et al, 1990). The biopharmaceutical company (R&D) report and the construction report (ERP) suggest that external support in the approach and reassessment of the situation are ways to reduce these perceived risks.

6. Conclusions

Cloud computing presents some important risks which should be assessed by any enterprise considering engagement in this area. Our main contribution consists of an empirical study of a sample of Swiss companies which is aimed at analyzing the understanding of the risks that public cloud services present and how they can be managed. Even though the sample size is very limited, we can see sufficient awareness of both the risks and the management solutions. The authors of the reports have consulted the large volume of literature pertaining to cloud computing risks with some of the reports referring to the Swiss regulatory context as well. There is also a degree of originality in the reports as they have considered the risks in the specific context of the concerned companies and according to their needs and capabilities.

As we could see, the detail and focus of the reports correspond to the particularity of the IT function to be migrated to the cloud. Therefore the reports were not just mere recounts of existing literature but show business awareness and planning capabilities. As far as the final recommendations of whether to go on the cloud are concerned, we find that they depend on the company's size, technological expertise and corporate culture but not on the criticality of the process or sensitivity of the data to be migrated.

The flexibility and cost-efficiency of the cloud should be more attractive to SMEs as compared to large companies. On the other hand, there may still be a certain level of mistrust in SMEs regarding the cloud as they lack sufficient expertise and risk management skills. Indeed, the reports suggest that large companies are better prepared toward the adoption of cloud services. Nevertheless, as this paper has shown, understanding, assessment and mitigation of the risks are vital when it comes to cloud computing. Once these steps have been properly addressed, where necessary with the help of external advice, the cloud may not look like such a dangerous place even for SMEs.

Finally, we stress again on the limited nature of our study whose purpose was to serve as an introductory exploration of the risk analysis with regard to prospective adoption of cloud services. Our findings cannot be extrapolated to all Swiss companies, but allow us to devise a stricter and more rigorous methodology for further studies based on interviews, questionnaires or quantitative surveys.

Vitae

Dr. Nathalie Brender, U.S. CPA (United States Certified Public Accountant), is a Professor of Risk Management, Accounting and Auditing at Haute Ecole de Gestion de Genève (HEG). She is currently teaching and conducting research in corporate governance, risk management, and in particular strategic risk management, and auditing. Her past professional experience includes management positions in business risk consulting, internal and external auditing, as well as financial reporting in the private sector.

Mr. Iliya Markov is a research assistant at Haute Ecole de Gestion de Genève (HEG). He has an MSc in operational research from the University of Edinburgh and a BA in mathematics and economics from the American University in Bulgaria. He has published several book chapters and articles. He is a recipient of awards and distinctions including an outstanding achievement in mathematics at the American University in Bulgaria. He is currently conducting research on corporate governance, risk management and operational research.

Highlights:

- We provide a definition of cloud computing and describe its main characteristics.
- We review the main risks associated with it and the relevant mitigation practices.
- We present reports on Swiss firms analyzing their prospective use of cloud services.
- There is a sufficient understanding of cloud-related risks and the appropriate controls.
- Firm size, expertise and needs influence the reports' analysis and recommendations.

References

Biswas, S. (2011a, January 20). Is cloud computing secure? Yes, another perspective [Web log post]. Retrieved from http://www.cloudtweaks.com/2011/01/the-question-should-be-is-anything-truly-secure (accessed on: January 25, 2012).

Biswas, S. (2011b, January 26). Computing without borders – What works, what doesn't [Web log post]. Retrieved from http://www.cloudtweaks.com/2011/01/computing-without-borders-what-works-what-doesn%E2%80%99t (accessed on: January 25, 2012).

Carroll, M., van der Merwe, A., & Kotzé, P. (2011, August). *Secure cloud computing: Benefits, risks and controls.* Paper presented at the 10th Annual Information Security for South Africa (ISSA) Conference, Johannesburg, South Africa. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6027519 (accessed on: January 3, 2012).

Cloud Security Alliance. (2010). *Top threats to cloud computing v1.0.* Retrieved from https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf (accessed on: December 12, 2011).

Cloud Security Alliance. (2011). *Security guidance for critical areas of focus in cloud computing v3.0.* Retrieved from https://cloudsecurityalliance.org/research/security-guidance (accessed on: January 6, 2012).

Cunningham, P. (2009, June). Three cloud computing risks to consider. *Information Security Magazine*. Retrieved from http://www.arma.org/press/armanews/infosecurity.pdf (accessed on: December 5, 2011).

Douglas, M., and A. Wildavsky (1983). Risk and culture : An essay on the selection of technological and environmental dangers. Berkeley ; Los Angeles: Univ. of California Press.

European Network and Information Security Agency. (2009a). *An SME perspective on cloud computing: A survey.* Retrieved from http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-sme-survey (accessed on: December 16, 2011).

European Network and Information Security Agency. (2009b). *Cloud computing: Benefits, risks and recommendations for information security.* Retrieved from http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment (accessed on: December 15, 2011).

Gartner, Inc. Gartner Says Worldwide Cloud Services Market to Surpass $109 Billion in 2012, http://www.gartner.com/newsroom/id/2163616.

Hawser, A. (2009). Cloud control. *Global Finance, 23*(11), 59-61. Retrieved from http://web.ebscohost.com/ehost/detail?vid=4&hid=122&sid=a0d05076-aae5-4452-83fd-b918d578dee0%40sessionmgr11&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=buh&AN=47598230 (accessed on: February 13, 2012).

Heiser, J., & Nicolett, M. (2008). *Assessing the security risks of cloud computing.* Stamford, CT: Gartner Research. Retrieved from http://cloud.ctrls.in/files/assessing-the-security-risks.pdf (accessed on: February 13, 2012).

Heskett, J., et al. (1990). Service breakthroughs: Changing the rules of the game. New York: Free Press.

Information Systems Audit and Control Association. (2010). *2010 ISACA IT risk/reward barometer – US edition.* Retrieved from http://www.isaca.org/About-ISACA/Press-room/Documents/2010-ISACA-Risk-Reward-Barometer-Results-US.pdf (accessed on: January 9, 2012).

Kaufman, L. M. (2009). Data security in the world of cloud computing. *IEEE Security & Privacy, 7*(4), 61-64. Retrieved from http://ieeexplore.ieee.org/search/srchabstract.jsp?tp=&arnumber=5189563&openedRefinements%3D*%26filter%3DAND%28NOT%284283010803%29%29%26searchField%3DSearch+All%26queryText%3DData+Security+in+the+World+of+Cloud+Computing (accessed on: December 4, 2011).

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing: Recommendations of the 33666 Institute of Standards and Technology.* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (accessed on: December 18, 2011).

OneStopClick. (2011). *Mobile & remote working in 2011: An overview of cloud services for today's SMEs.* Retrieved from http://hosting.onestopclick.com/white-papers/129/mobile-remote-working-in-2011-an-overview-of-cloud-services-for-today%E2%80%99s-sme.html (accessed on: January 8, 2012).

Popovic, K., & Hocenski, Z. (2010). Cloud computing security issues and challenges. *Proceedings of the 33rd International Convention MIPRO,* 344-349. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5533317 (accessed on: January 8, 2012).

Prakash, S. (2011, March/April). Risk management: Cloud computing considerations. *Canadian Management Accounting*. Retrieved from http://www.nxtbook.com/nxtbooks/naylor/SMAS0211/index.php#/40 (accessed on: February 2, 2012).

Scheier, R. L. (2009). *What to do if your cloud provider disappears.* Retrieved from http://www.infoworld.com/d/cloud-computing/what-do-if-your-cloud-provider-disappears-508?page=0,3 (accessed on: February 2, 2012).

Sultan, N. A. (2011). Reaching for the "cloud": How SMEs can manage. *International Journal of Information Management,* 31, 272-278. Retrieved from http://web.ebscohost.com/ehost/detail?vid=7&hid=9&sid=a0d05076-aae5-4452-83fd-b918d578dee0%40sessionmgr11&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=buh&AN=59953059 (accessed on: January 10, 2012).

Sultan, N. A. (2010), Cloud Computing in Education: A New Dawn?, *International Journal of Information Management.* 30, 109-116.

Treasury Board of Canada Secretariat. (2010). *Guidance on preparing information sharing agreements involving personal information.* Retrieved from http://www.tbs-sct.gc.ca/atip-aiprp/isa-eer/isa-eer01-eng.asp (accessed on: January 25, 2012).

Zekrya, M. (2011, November). *Le cloud computing en Suisse: Résultats de l'enquête auprès des entreprises: Course notes* [PowerPoint slides]. Geneva: Haute Ecole de Gestion.