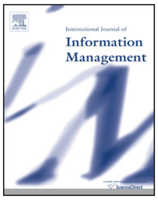
International Journal of Information Management 33 (2013) 726–733

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt



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

Nathalie Brender[1], Iliya Markov*

Haute Ecole de Gestion de Genève, Campus de Battelle, Bâtiment F, 7 route de Drize, 1227 Carouge, Switzerland

ARTICLE INFO

Article history:
Received 22 March 2012
Received in revised form 22 February 2013
Accepted 15 May 2013
Available online 14 June 2013

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

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.

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.

* Corresponding author. Tel.: +41 22 388 17 27; fax: +41 22 388 17 01.
E-mail addresses: nathalie.brender@hesge.ch (N. Brender), iliya.d.markov@gmail.com (I. Markov).
[1] Tel.: +41 22 388 18 72; fax: + 41 22 388 17 01.

0268-4012/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ijinfomgt.2013.05.004

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