Government Information Quarterly 27 (2010) 245–253

Contents lists available at ScienceDirect

Government Information Quarterly

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

Identifying the security risks associated with governmental use of cloud computing

Scott Paquette [a,*], Paul T. Jaeger [b], Susan C. Wilson [b]

[a] College of Information Studies, University of Maryland, College Park, MD 20740, USA
[b] University of Maryland, College Park, MD, USA

ARTICLE INFO

Available online 13 April 2010

Keywords:
Cloud computing
Risk management
IT security
IT governance
Grid computing
Governmental computing

ABSTRACT

Cloud computing, which refers to an emerging computing model where machines in large data centers can be used to deliver services in a scalable manner, has become popular for corporations in need of inexpensive, large scale computing. Recently, the United States government has begun to utilize cloud computing architectures, platforms, and applications to deliver services and meet the needs of their constituents. Surrounding the use of cloud computing are many risks that can have major impacts on the information and services supported by this technology. This paper discusses the current use of cloud computing in government, and the risks–tangible and intangible–associated with its use. Examining specific cases of government cloud computing, this paper explores the level of understanding of the risks by the departments and agencies that implement this technology. This paper argues that a defined risk management program focused on cloud computing is an essential part of the government IT environment.

1. Introduction

Cloud computing, which allows for highly scalable computing applications, storage, and platforms, is increasing in importance throughout government information technology (IT) strategy. Cloud computing providers offer a variety of services to individuals, companies, and government agencies, with users employing cloud computing for storing and sharing information, database management and mining, and deploying web services, which can range from processing vast datasets for complicated scientific problems to using clouds to manage and provide access to medical records (Hand, 2007). Recently, President Barack Obama and Chief Technology Officer (CTO) Vivek Kundra have both expressed the vision to explore the cloud as a key component in the federal IT transformation, and therefore agency use of cloud computing capabilities has increased (Jackson, 2009; Miller, 2009b).

Although many benefits are reported in cloud computing use, a great deal of risk is associated with the implementation, management, and use of cloud computing technologies. In a government context, both tangible risks (such as the risk of unauthorized access, infrastructure failure, or unavailability) and intangible risks (such as confidence in the technologies capabilities, and public access) are introduced along with the functionality and benefits provided by cloud applications. The government's ability to manage these risks will be a key determinant in the success of cloud computing.

This paper discusses the nature of cloud computing and risk management in a governmental context. The risks associated with cloud computing are identified, focusing on both the tangible and intangible risks which can present challenges for IT management. We argue that much evidence exists that cloud computing has become a strategic direction for many government agencies and is already employed in critical areas of the government's IT infrastructure. However, a prudent and in-depth risk management program must accompany the use of this new technology in order to prevent unwanted technical consequences, and even greater problems from a government information management perspective.

2. The nature of risk and risk management

The word "risk" is derived from the Italian *risicare*, which translates to English as "to dare." At the origin of the word is the implication that risk is not a fate, but a choice individuals make depending on internal or personal factors, and the environment in which we live (Bernstein, 1998). Others define risk as the possible impact or result of an event on assets of an organization, and the corresponding consequences that occur (Stoneburner, Goguen & Feringa, 2004). Risk is not defined or classified by the size of the risk, but by the balance of expected and unexpected consequences. In economic terms, this is known as "value at risk," which is a statistical measure that defines the consequence of a loss by the chance of occurrence or confidence level (Crouhy, Galai & Mark, 2006).

A basis for all discussions of risk is its relationship to the idea of reward. This concept is easy to define and observe with risks associated with market-tradable instruments, as a cost of the risk is determined by the market and is easily compared to the expected rewards. More often, a challenge exists for organizations when the risk cannot be associated with a well-understood or widely-accepted cost. In this case,

* Corresponding author.
E-mail addresses: spaquett@umd.edu (S. Paquette), pjaeger@umd.edu (P.T. Jaeger), scwilson@umd.edu (S.C. Wilson).

0740-624X/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.giq.2010.01.002

organizations are susceptible to engaging in high-risk activities that may yield short-term benefits based on a misunderstanding or ignorance of the risk involved and the unrealistic rewards. It is because of this particular failure in managing risk that organizations develop risk management programs in order to identify, mitigate, and manage risks to achieve acceptable rewards (Crouhy et al., 2006).

Risk management is "the process of understanding, costing, and efficiently managing unexpected levels of variability in the financial outcomes for business" (Crouhy et al., 2006, p. 8). It includes the activities involved in selecting and implementing mitigation measures to bring risk to an acceptable level within an acceptable cost. Here, the important term is "acceptable," which must be defined based on a risk-reward framework which will encompass the value of a particular asset, and the consequence for its loss (both from a short-term and long-term perspective). Risk management is not a defensive activity, but the process of developing a risk-adjusted strategy that balances opportunity with consequence of actions (Crouhy et al., 2006).

Included in any definition of commercial or public-sector risk are the risks associated with information, information systems, and technology. These system risks are of special interest to those who are charged with the management and operation of an organization's information technologies. Systems risks are potential system losses, breaches, or failures which may mean "modification, destruction, theft, or lack of availability of computer assets such as hardware, software, data, and services" (Straub & Welke, 1998, p. 442). Common examples of identified systems risk might include computer abuse and misuse, disaster scenarios realized, violations of access restrictions, and exposure of intellectual property resident in computer systems. Systems security risk, a subset of systems risk, refers to a situation wherein the firm's information or information system technology are not sufficiently protected against damage or loss (Straub & Welke, 1998).

In regard to these systems risks, the U.S. Department of Commerce states that the purpose of maintaining a systems-focused risk management program is to

1) Better secure information technologies that process organization information;
2) Provide the necessary information to management in support of decision making surrounding the deployment of IT assets; and
3) Support management's authorization or accreditation of IT based on risk-focused assessments (Stoneburner et al., 2004).

Further, "risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions" (Stoneburner et al., 2004, p. 6). Most risk management programs exist in organizations through being tightly tied to a standard system's development life cycle (SDLC) in order to manage risk at all stages of technology development and deployment.

Outsourcing is a strategy for managing the risk of information technologies in organizations that has recently become popular. A key benefit as purported by advocates of outsourcing is the ability of the client and the vendor to share both the risks and rewards of their information technology. In fact Dibbern, Goles, Hirschhiem and Jayatilaka (2004) state "due to vendor opportunism … some companies have formed relationships with multiple vendors in order to mitigate the risks" of IT deployment (p. 32). IT managers often claim that outsourcing their information systems reduces the technological risk and uncertainty that would have been managed by an organization (Clarke, Zmud & McCray, 1995) at their time and expense and likely, outside of the organization's core competency.

To understand the risks associated with outsourcing related activities, "it is essential to identify the array of potential undesirable outcomes that could occur with respect to the outsourcing arrangement" (Aubert, Patry & Rivard, 2005, p. 12), which can be expressed by the magnitude of losses and the probability of such an occurrence. Even though risk management entails a high level of complexity and the conclusions reached are sometimes far from precise, identifying the risks of outsourcing allows the risk to be managed. These findings can become the basis for managing the risk surrounding one particular type of IT outsourcing, the use of the cloud.

3. What is cloud computing

Cloud computing refers to an emerging model of computing where machines in large data centers can be dynamically provisioned, configured, and reconfigured to deliver services in a scalable manner, for needs ranging from scientific research to video sharing to e-mail (Wyld, 2009). While usually described as a single entity, cloud computing can comprise several components at once: cloud infrastructure, cloud platform, and cloud application. *Cloud infrastructure* is the provision of a computer infrastructure as a service–both computational resources and storage–such as Amazon's Elastic Compute Cloud (EC2) and S3 services (Youseff, Butrico, & Da Silva, 2008). This infrastructure allows users to configure the infrastructure themselves, including the rapid expansion of their infrastructure based on network requirements. *Cloud platform* is the provision of a computer platform or software stack as a service, such as Google's App Engine or Salesforce.com. *Cloud applications* are web services that run on top of a cloud platform or infrastructure and are made available to the organization's users or customers. They can include applications that are commonly known to the public including YouTube's video hosting applications and Google's GoogleDocs set of office applications.

Cloud providers already offer a variety of services to individuals, companies, and government agencies, with users employing cloud computing for storing and sharing information, database management and mining, and deploying Web services that can range from processing vast datasets for complicated scientific problems to using clouds to manage and provide access to medical records (Hand, 2007). The incredible level of information and processing capacity level of data available in the cloud–the petabyte scale–allows for entirely new approaches to data analysis (Anderson, 2008). Individuals may use cloud computing simply to store e-mail and other documents, where large corporations and scientists can use the vast computing power available to add a new dimension to their current IT infrastructure (Wyld, 2009).

Cloud computing opens up the possibility that a major cloud provider such as Google could ultimately become "the world's primary computer" (Baker, 2007, para. 5). Cloud computing represents a centralization of information and computing resources–quite contrary to the imagery that the label evokes–and many individuals, corporations, and government agencies are already frequent or constant, though often unknowing, users of cloud computing. The speed at which cloud computing has permeated Internet activities is increasing exponentially. Although many users may not be familiar with the term, the reality is that most users are already taking advantage of the cloud through Web-based software applications and on-line data storage services, like Google, YouTube, and Flickr (Buyya, Yeo & Venugol, 2008; Horrigan, 2008).

The notion of cloud computing not only changes an organization's infrastructure, but how they do business. As federal CIO Vivek Kundra has stated, " … it's a fundamental change to the way our government operates" (Wyld, 2009, p. 16). Accordingly, the federal government has already begun to implement cloud computing within their IT strategies. In early 2009, the General Services Administration (GSA) announced that the primary e-Government portals–USA.gov and its Spanish-language companion site, GobiernoUSA.gov–would be supported by cloud computing contracted with Terremark Worldwide's proprietary Enterprise Cloud platform (Beizer, 2009; Kash, 2009). Further, the Obama Administration has also expressed interest in the large-scale use of cloud computing for government storage and processing ("Will cloud computing work in the White House, 2009).