Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Selecting a trusted cloud service provider for your SaaS program

Changlong Tang[*], *Jiqiang Liu*

Institute of Information Science, Beijing Jiaotong University, Beijing 100044, China

ARTICLE INFO

Article history:
Received 28 August 2014
Received in revised form
26 December 2014
Accepted 6 February 2015
Available online 19 February 2015

Keywords:
SaaS
Software as a service
Cloud security
Trusted cloud services
Function
Auditability
Governability
Interoperability
Security assurance

ABSTRACT

Software as a Service (SaaS) offers major business and IT benefits that organizations are looking to take advantage of. SaaS adoption presents serious and unique security risks. Moving a company's sensitive data into the hands of cloud providers expands and complicates the risk landscape in which the organization operates.

This paper highlights the significance and ramifications of a structured selection of a Cloud Service Provider (CSP) in achieving the required assurance level based on an organization's specific security posture. This paper proposes a holistic model, known as the Function, Auditability, Governability and Interoperability or FAGI, as an approach to help a Cloud Service Consumer (CSC) to engage and select a trusted CSP through four major decisions: Selecting a safe cloud that has adequate security functions; Choosing an auditable cloud via third-party certifications/assessments or self tests; Picking out a governable cloud that provides the required transparency; Opting for a portable cloud that ensures the desired portability.

A case study reveals the FAGI approach offers an objective and efficient way to choose a qualified and trusted cloud service and in turn saves CSCs' time, effort, and grief.

1. Introduction

Cloud computing is not just a trend anymore. The cloud has changed how enterprises design and deliver applications. This change in application design and delivery has altered where information is stored, how it is accessed, and how it is managed (KMPG, 2011). Organizations are planning to, or have already started, to integrate cloud into their organizations' IT systems due to the extremely compelling cost-saving potential for cloud based deployments (Joyent, 2012). The benefits from cloud (especially SaaS) include: reduced time to value, increased connectivity, lower cost, scalability, integration and ease of use.

The benefits need to be balanced by the potential risks that come from cloud computing. The primary risk comes from the very nature of cloud services: the co-localization of large amounts of valuable data. Criminal attackers can go directly to one source for multiple corporation and users sensitive data rather than attacking multiple networks and users. For the cloud to reach its incredible potential, business cloud customers must address security gaps that represent significant threats, especially to large organizations and those in heavily regulated industries in order to securely realize the full IT and business benefits available.

A whole spectrum of new risks and threats exist in the cloud that were not present on traditional on-premise based

* *Corresponding author*. Unit 301, 115 Cherryhill Blvd. London, ON N6H 2L8, Canada. Tel.: +1 1226 376 5251.
E-mail address: AlanTang.it@gmail.com (C. Tang).
http://dx.doi.org/10.1016/j.cose.2015.02.001
0167-4048/

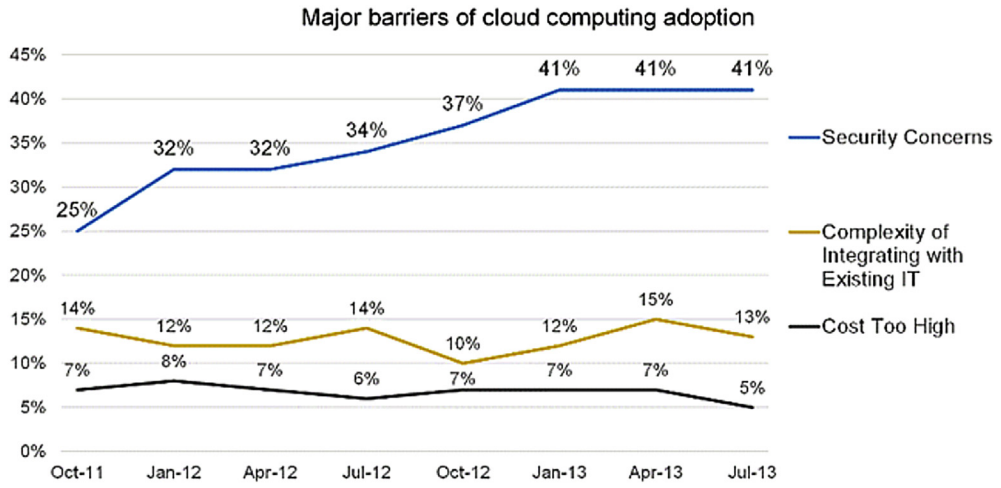

Fig. 1 – Barriers of cloud computing adoption. Note: color on the Web only.

networks. Although the security capabilities for SaaS applications have developed greatly they are still in flux with no standards for individual organizations to build their information security. In many cases, information security has proven to be one of the major barriers to cloud adoption as shown in Fig. 1 (ChangeWave Research, 2013).

The role of the Chief Information Security Officer (CISO) is changing. Traditional responsibilities of securing on-premise infrastructure, applications, people, and processes are moving into hybrid and cloud environments requiring different strategies and techniques. Conventionally, security was seen as a technical requirement of the SaaS program. The ability to protect critical data is becoming a part of business goals and objectives (Dimension Data, 2012).

Understanding the interaction of cloud computing and the regulatory environment is a key component of any cloud strategy. General perceptions around cloud security are an aggregate of specific concerns (HiMSS, 2012). The ability to vet those out may disperse some perceived concerns in lieu of the truth: the cloud can be secure. More and more people are demanding SaaS programs today causing security standards to mature and become commoditized (CloudComputingAdmin, 2014). Also, many organizations do not realize that the cloud does not just bring security

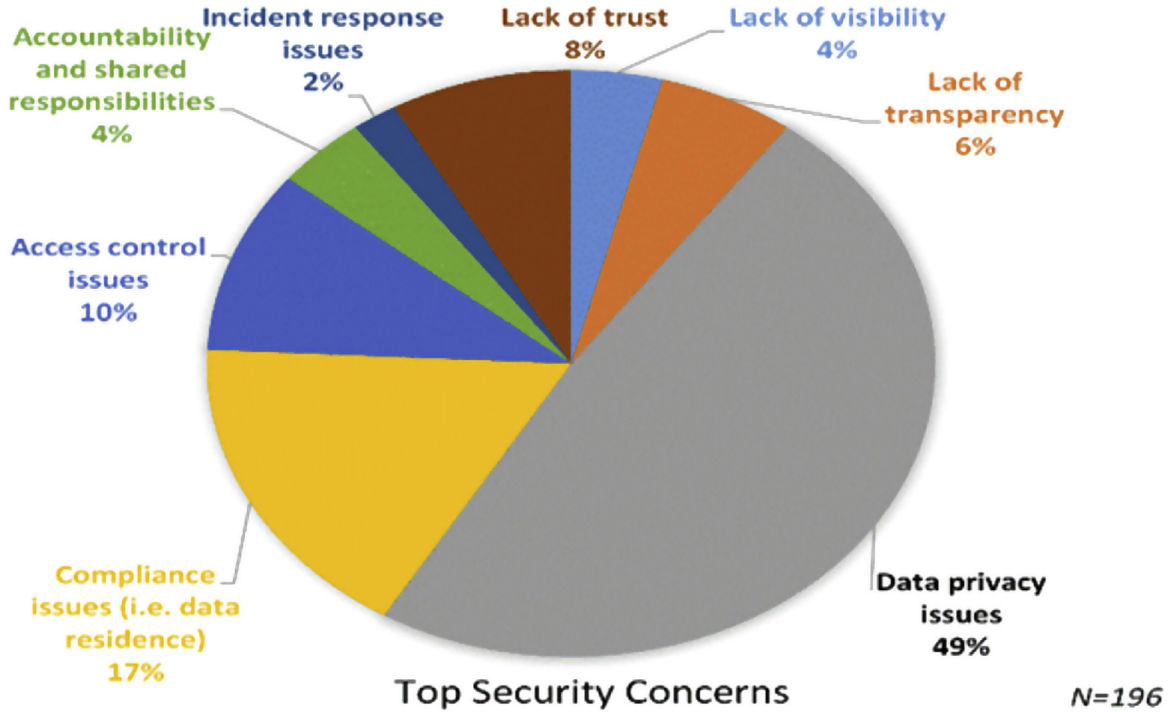

Fig. 2 – Top security concerns of SaaS. Note: color on the web only.