Chapter 15

Enterprise IT Transformation
Using Cloud Service Broker

Rajesh Jaluka
IBM Corporation, USA

ABSTRACT

Cloud is significantly changing the economics as well as delivery and support model for Information Technology. Every enterprise needs to come up with a plan to transform their current IT and embrace cloud. The road to transformation poses many challenges and there is no one right answer. The objective of this chapter is to describe some of the key challenges and provide a methodology based on IBM Design Thinking to address the challenges. The author will also enlighten the readers on how a Cloud Service Broker can help smoothen the journey.

INTRODUCTION

Large and medium enterprises have developed a large number of IT systems over several decades. Many of these systems are complex and involve many components. These systems support mission critical functions. Uprooting these systems from the current on-premises datacenter and moving them to a cloud environment is complicated and involved. For example, a survey found 48% of businesses and government organizations continue to rely heavily on COBOL and many of these applications are two decades old (Fiscutean, 2015). The application owners need to take into account factors like migration cost, differences in technology stack, the skills of its technical staff, software licensing, security, supportability, availability, recoverability, and total cost of ownership. Furthermore, the enterprises are building new services on cloud that will need to work seamlessly with their existing systems.

Security and data privacy remain the biggest barriers to the adoption of cloud. On the commercial front, any extended downtime or security breach can severely impact customer satisfaction, lead to customer attrition, affect revenue or even tarnish a company’s reputation. One such recent (May 21, 2015) example is Apple iCloud outage that affected 200 million users (Kelly, 2015). The outage lasted seven hours and affected 11 services including email, calendar, and reminders. A similar outage in March
2015 cost Apple $9.12 million (Geier, 2015). However, when the breaches happen on the social front the impact is much wider.

The attack on Anthem, a U.S. health insurance provider, in February 2015 potentially exposed social security numbers, addresses, phone numbers, email addresses, employment data and income data of 80 million patients and employees (Terhune, 2015). Another such attack on the U.S. Office of Personnel Management compromised data of 21.5 million federal workers (Scuitto, 2015). These attacks can lead to citizens’ call for stricter laws and regulations. These laws and regulations can severely restrict what services can be consumed from cloud and how they are consumed. For example, data residency laws will limit enterprises and agencies to only those service providers that have presence in the country or the region. Similarly, these attacks can also lead to geopolitical tensions between countries. In the U.S. Office of Personnel Management case, the initial reports have tied the attacks to China-based hackers. Such instances can lead to new laws and regulations that may require enterprises to react quickly to comply with these laws and regulations. Service providers, too, can impose self-regulations to promote an underserved social cause or take a moral stand.

To address such concerns, service providers have come up various designs to implement cloud e.g. public cloud, private cloud, and hybrid cloud. A hybrid cloud uses private cloud infrastructure in combination with public cloud services. It is possible for very small businesses to have all its IT needs completely served through public cloud service providers. However, most medium and large enterprises will continue to have compute resources in its traditional data centers for many years to come and will combine it with private and public clouds from multiple service providers. According to IBM (n.d. a),