Benefits and risks of cloud computing

Stephen Turner
Known-Quantity.com and Holy Family University

ABSTRACT

Cloud computing vendors maintain data away from the facilities of their customers. This is compelling because it enables companies to focus on what they do best and leave the technology to outside specialists. Many service providers offer metered service – much like a utility. This model is attractive to smaller organizations that are looking to remain flexible in a challenging economic climate and contain costs. Price alone is only one component of the total cost of ownership (TCO). Larger organizations are looking at factors such as adoption costs, training, downtime, regulatory implications, data security risks and how a change might jeopardize trade secrets. As a result, many larger organizations are more reluctant to move to the cloud.

During the decision-making process, information systems management professionals should also consider how the technology will serve the needs of the organization and it management. After making the decision to proceed with cloud computing, it is critical that a client negotiate an enforceable contract with the service provider, anticipating things like technology failure and even bankruptcy. The agreement should define who owns, accesses and controls data, where it is actually housed and how often it is backed-up. This can mitigate risks inherent to cloud computing.

KEYWORDS

Cloud computing, business model, total cost of ownership, adoption costs, legal implications, contract negotiations

INTRODUCTION

More organizations are choosing to use cloud computing. Global revenue is expected to reach $149 billion by 2014.1

However, the cloud is not displacing legacy systems in all cases. Traditional client/server computing, enterprise computing and mainframes are expensive to maintain, yet some information systems professionals with some larger organizations have decided the change may not be worth the adoption costs and risks to make the conversion to the new model.

Small and mid-sized businesses may already need to make upgrades, so the cloud has been a good option to consider at that stage – especially because of the pricing and scalability. It allows them to move some or all of their data storage computing needs out of their facilities, make upgrades and avoid large upfront expenditures.

Cloud computing offers measured service, much like a utility. This model is particularly cost-effective as demand levels change. Some organizations may only need cloud infrastructure as service, while some of their departments may also need platform and/or software to address needs at a given time. 2

This business model is compelling because it rarely locks customers into a long-term commitment and high fixed costs.

BUSINESS MODEL

Paul Weifels, of the Chasm Group, has stated that a successful business model depends on achieving the "means to create, deliver and communicate the value that customers are looking for." 3

A cloud service provider dedicates many servers to support data needs of clients, which allows it to grow rapidly if those needs increase. It also spreads the costs among several clients. Proponents and analysts have successfully communicated the value this creates for customers. Management pays close attention to the value and impact on strategy.

A global recession has necessitated cost-cutting among many companies. Cloud computing came along at the right time, but the monthly fee is not the only cost to consider. The decision to make the change should factor-in several items, including total cost of ownership (TCO).

With cloud computing, TCO does not actually include ownership, just total cost. Therefore, there are no hardware or software acquisition costs, maintenance or expenses for space and energy. There may be costs for training, support and downtime. In particular, downtime may not be acceptable to some businesses.4

RISK ASSESSMENT

Organizations with a need for the highest level of uptime should be skeptical as they evaluate cloud computing, especially if they already have systems in place that may be more reliable than cloud computing. One metric to consider in evaluating a cloud vendor is their downtime history.

If certain functions are mission-critical, cloud computing may not be the complete solution. For such organizations, a hybrid model may be beneficial. Non-mission-critical functions could be performed on the cloud. A hybrid model can also introduce mobile access without applying it universally throughout an organization.

Other organizations have security and regulatory compliance requirements to satisfy. For example, University of Wisconsin developed guidelines to comply with the Health Insurance Portability & Accountability Act of 1996 (HIPAA). Specifically, it requires that certain IT staff – only those with related responsibilities – are able access server rooms or remove equipment. 5 Cloud computing does not comply with these guidelines.

This is true for health records at University of Wisconsin, but may not apply to student records. Therefore, cloud computing is not applicable for some departments (such as hospitals and health systems), while it may serve other departments (such as the registrar).

Therefore, this type of decision must factor-in the nature of the organization and its departments.

Different challenges dictate different solutions. There are certain organizations that simply cannot afford to have security breaches. These destroy trust. In April 2011, Epsilon had "unauthorized entry" to about fifty client accounts that were managed on the cloud. Each account may contain thousands of email addresses – Epsilon is an email marketing company. The clients in turn, had to face the music with their own customers; many are financial institutions. Not good for banks and not good for the reputation of cloud computing. As a result, some organizations are rethinking their choices.6

Buyers and sellers of technology have the responsibility to discuss the limits of what it can do and when not to use it. These decisions cannot be made in isolation and are indeed informed by an understanding of management and organizational needs. This understanding empowers information systems influencers and buyers to look at acceptable alternatives.

Rather than using a public cloud, an alternative is a private cloud. These are deployed on a proprietary basis and apply many of the same principles as public cloud computing. Private clouds are considered more secure.7

Officials are already using private clouds in the U.S. Federal Government to manage highly confidential information. However, they are re-evaluating how to improve security.8

The Government Accountability Office (GAO) studied security incidents in 2010 on Federal information systems. The results of the study were alarming. Malicious code was placed on computers or systems in 30% of cases. Other top incidents included investigation, improper usage, unauthorized access and scans/probes/attempted access.9

Government information systems are not all the same. Not all hold classified national security information, but most do contain sensitive data.

Private sector information systems can also hold very sensitive information. As a result, private enterprise must also consider legal implications. According to the law firm Hogan Lovells, when it comes to "compelled disclosure" to authorities, information stored on the cloud is subject to different protections than data retained on in-house storage devices and servers. As a result, a company's data could be accessed by the government through the cloud service vendors using warrants and subpoenas – without

the owner of the data being informed or having standing in the action. Information stored on a "remote computing service" that is older than 180 days is also subject to search by authorities with just an administrative subpoena.10

If a company has trade secrets, a private cloud is an option, but the vendor needs to specify what steps will be taken to keep them secure. Cloud computing providers need policies to address what will happen in the event of subpoenas, attempted intrusions or other threats. They also need to set policies and assure that staff members and sub-contractors who access the data and devices that store the information are maintaining the security of the secrets. If sufficient measures are not taken, a business may lose protection of their secrets on the cloud. Keep in mind that states have jurisdiction over trade secrets.

Many decisions are made without considering legal issues associated with the cloud. And vendors don't always disclose what kinds of problems have been faced by other customers already using their technology.

System Solution, Inc. (SSI) is a technical support and cloud vendor for many clients. SSI was providing service an on-site server and network for non-profit management and fundraising business. In 2009, SSI provided a proposal to save the client money over the long-term by switching to a private cloud – a server in a data center. SSI provided the reassurance that they understood the need of the client and would evolve services to meet the changing demands. As a result, the client became an early adopter of cloud systems. The client was not told that there could be downtime and did not know to ask about the potential risks or legal implications.

For the most part, service has been reliable, but there have been more problems than there ever were before moving to the cloud, which has interfered with fundraising and other activities and resulted in lost opportunities and funding. The service has gone down on number of instances, and SSI blamed either the client's staff for over-utilizing the service or the internet service provider for FiOS interruptions. There was also an air conditioning failure at one of the server farms it uses and servers overheated and burned-out, causing the loss of data and email messages. Expectations of cost savings have not been met with the reality, when you look at the actual TCO.

TECHNOLOGY, MANAGEMENT AND ORGANIZATION

Before making a decision whether to move to the cloud for part or all of a company's infrastructure, platform or software, an information systems professional should look at the management, organizational and technology needs in greater detail.

Management has the responsibility of setting organizational strategy, which will determine the nature of information systems required. Strategy will dictate which functions are mission-critical.

The organization itself may or may not be well-suited to make the change, by virtue of privacy, security, legal and other requirements. Organizations are capable of adapting, but the extent and costs of change in adopting the cloud should be identified in advance. The organization should also consider communicating plans to use the cloud to partners and constituents, so that they can also understand their risks.

The exact technology solution must satisfy the needs of management and the organization. It must offer a solution to a business problem and address business

challenges.11 Not all vendors offer the same solutions, and not all organizations or departments have the same needs.

CONTRACT NEGOTIATIONS

If your organization makes the decision to move to the cloud, a detailed contract is needed to define what it is really getting. An agreement should include provisions that will define service levels, what will happen if the vendor fails to deliver and how your data will be protected.

A buyer should know where the data itself is stored. If your organization is based in the United States, the data should be housed domestically. This will provide you with a way to enforce the contract in U.S. courts. Also, define where data back-up is maintained – assuring that it is in a different domestic location. If you can't afford to lose data, you should also specify how frequently the vendor will monitor the back-up to see if there are errors. This will minimize the chance that data will be lost altogether.

The contract could also require a bond or insurance policy that will pay for recovery of data and all the other costs that might arise if there is a failure and the vendor cannot or will not pay for what you need.

The vendor should also commit to some kind of a periodic information audit by a third party, who can confirm that various obligations are being met.

All of the additional measures defined in the contract can be expensive and may push the TCO beyond what it costs to maintain information at your own facilities.

CONCLUSION

Cloud computing is not completely reliable and has many risks. Yet, the cloud model might be acceptable to organizations concerned more about costs than the value of their information. It is particularly compelling for organizations with no trade secrets, sensitive data or compliance requirements.

Information and intellectual property are your most valuable assets. A risk/benefit analysis is well worth the time before you hand over those assets to a third party.

CITATIONS AND REFERENCES

1. Kenneth C. Laudon, Jane C. Laudon, *Management information systems, managing the digital firm*, 12th Edition (Upper Saddle River, New Jersey: Pearson Prentice Hall, 2012), 170.

2. Ibid, 183

3. Stephen Turner, Stan DeVaughn, *NET value: How the digital culture changes your value proposition* (San Francisco: Turner DeVaughn, 2008), 106 (see Business Model Innovation, Expert Insight by Paul Weifels)

4. Kenneth C. Laudon, Jane C. Laudon, *Management information systems, managing the digital firm*, 12th Edition (Upper Saddle River, New Jersey: Pearson Prentice Hall, 2012), 196.

5. Milford & Hutton, *HIPAA Security Best Practices Guidelines* (Madison, Wisconsin: University of Wisconsin-Madison, April 15, 2005) 3-4
Retrieved from http://hipaa.wisc.edu/docs/serverSecurity.pdf

6. Fahmida Y. Rashid, "Epsilon Data Breach Highlights Cloud-Computing Security Concerns," eWeek April 6, 2011
Retrieved from http://www.eweek.com/c/a/Security/Epsilon-Data-Breach-Highlights-Cloud-
Computing-Security-Concerns-637161/

7. Kenneth C. Laudon, Jane C. Laudon, *Management information systems, managing the digital firm*, 12th Edition (Upper Saddle River, New Jersey: Pearson Prentice Hall, 2012), 183

8. C-Span, "House Homeland Security Hearing on Cloud Computing," Thursday, October 6, 2011
Retrieved from http://www.c-span.org/Events/House-Homeland-Security-Hearing-on-Cloud-Computing/10737424626/

9. Government Accountability Office, "*GAO-12-137 information security: weaknesses continue amid new federal efforts to implement requirements*" October 3, 2011
Retrieved from http://www.gao.gov/htext/d12137.html

10. Hogan Lovells, Privacy and Information Management Practice / Washington, DC, "*Cloud computing: A primer on legal issues, including privacy and data security concerns*," slides 4, 6
Retrieved from
http://www.cisco.com/web/about/doing_business/legal/privacy_compliance/docs/CloudPrimer.pdf

11. Kenneth C. Laudon, Jane C. Laudon, *Management information systems, managing the digital firm*, 12th Edition (Upper Saddle River, New Jersey: Pearson Prentice Hall, 2012), 81