pillsbury

IS YOUR HEAD IN THE CLOUDS YET? THE TOP 10 ISSUES YOU NEED TO KNOW ABOUT CLOUD COMPUTING

By Marla A. Hoehn and John L. Nicholson[1]

One of the hottest buzzwords in technology today is "cloud computing." While there is sufficient debate about what exactly "cloud computing" means, at the core is one party (the customer) obtaining information technology (IT) services from a someone else (the provider). In the broadest sense, cloud computing means a provider assembling the infrastructure and capability to provide large-scale IT services to numerous customers simultaneously, and it includes such things as data storage and processing and delivery of software as a service (SaaS).[2] According to the marketing hype, cloud computing frees companies from the need to buy hardware and software and maintain their own IT infrastructure, making them more nimble and better able to adapt to changing market demands, not to mention curing the common cold. Unfortunately, as roughly 7500 customers of online backup and storage provider Carbonite, Inc. learned recently,[3] "cloud computing" has some of its own issues and risks.

In some ways, cloud computing deals are the same as any other type of service arrangement – you're contracting for a service, negotiating terms and conditions, SLAs and pricing, and making sure that what the supplier is providing is the service you actually think you're getting. However, due to the nature of cloud-based services, there are a handful of issues that should specifically be considered and resolved as part of the agreement between the parties before the relationship begins in order to avoid unpleasant and unexpected consequences:

1. **Privacy and Security** –

"When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else." – David Brin

Privacy and security issues are typically at the top of the list when considering cloud computing issues, and those concerns become even more important for companies in the health care industry. These twin issues are primary reasons many entities, particularly large ones, may be reluctant to adopt cloud computing. In some cases and for certain services, companies will opt

---

[1] Marla Hoehn is a partner with Pillsbury Winthrop Shaw Pittman, LLP, and is based in the firm's Silicon Valley office. More information about Ms. Hoehn's practice is available at http://www.pillsburylaw.com/marla.hoehn. John Nicholson is a counsel with Pillsbury and is based out of the firm's Washington, DC, office. More information about Mr. Nicholson's practice is available at http://www.pillsburylaw.com/john.nicholson.

[2] Eric Knor & Galen Gruman, *What Cloud Computing Really Means*, INFOWORLD, April 07, 2008, http://weblog.infoworld.com/archives/emailPrint.jsp?R=printThis&A=/article/08/04/07/15FE-cloud-computing-reality_1.html.

[3] See "Data backup firm sues 2 hardware suppliers," Weisman, Robert, Boston Globe, March 21, 2009, available at http://www.boston.com/business/technology/articles/2009/03/21/data_backup_firm_sues_2_hardware_suppliers/ (last visited March 23, 2009).

against using cloud services altogether because of these issues.[4] But for some types of services, cloud computing may make sense if the privacy and security risks can be mitigated.

At the forefront of the customer's mind is, who can access and use my data? A related issue is what rights, if any, does the provider reserve to use the customer data. Also, what level of security is the provider willing to provide? Is the provider's service consistent with my privacy policy? Will the data be encrypted? Details about these issues should be included as part of the contract, whether in the main body or in attachments. One way for providers to assure customers that they are taking security seriously is for the provider to be compliant with one or more of the relevant ISO 27000-series of information security standards.[5]

One significant concern for companies with multinational operations considering a cloud-based service is compliance with the European Data Protection Directive (the "EU Directive"),[6] which requires a "data controller" to ensure that any third party "processing" personal information in the EU (or exported from the EU) implements adequate organizational and technical security measures to protect the data. The EU Directive restricts companies from exporting personal information outside the EU to any country that does not have, in the EU's opinion, "adequate" data privacy laws (the US does not), unless certain specific requirements have been met. Many other countries have implemented data protection laws modeled after the EU, so companies considering the cloud services model, in general, and those with international operations, in particular, need to consider whether the provider's operating model creates cross-border data privacy issues. One particular issue to consider is the requirement in the EU and other countries with similar privacy laws that data controllers comply with "fair information practices," which include allowing data subjects to be informed of, and have an opportunity to consent to, the location where their data is processed and any parties (e.g., subcontractors) that might have access to the data. In a cloud services model, such compliance with fair information practices can be challenging, at best.

Once the data is in "the cloud," what happens if it is somehow disclosed to unauthorized individuals? Many states have laws requiring certain protective measures for the security of personal information and/or requiring that if a security breach of certain personal information occurs, notice must be given to the affected individuals.[7] If the provider and the customer are located in different states, which state's law governs with respect to the customer's data hosted

---

[4] For interesting discussions of which applications seem most suited for the cloud, see Ephraim Schwartz, *The Dangers of Cloud Computing*, INFOWORLD, July 07, 2008, http://www.infoworld.com/article/08/07/07/28NF-cloud-computing-security_1.html; and Galen Gruman, *Early Experiments in Cloud Computing*, INFOWORLD, April 07, 2008, http://www.infoworld.com/article/08/04/07/15FE-cloud-computing-utility_1.html.

[5] For a general description of the ISO 27000-series of standards, see http://www.27000.org/index.htm (last visited March 24, 2009).

[6] EC/95/46.

[7] An early example is the "California Security Breach Information Act" S.B. 1386, (Cal. 2003). More recently, broad and stringent security breach law and regulations have been passed and are being implemented in Massachusetts. "Standards for the Protection of Personal Information of Residents of the Commonwealth." 201 Mass. Code Reg. Section 17.00.

by the provider?[8] What if the data itself is located in yet another jurisdiction? What if the legal obligations of the provider and customer conflict? Because of these issues, it is important for both the provider and the customer to understand their own respective legal obligations with respect to the data in the cloud, to know what terms in the service agreement it can and cannot agree to. For example, if the provider is obligated to give notice to appropriate authorities and individuals of a security breach, the customer will want, to the extent permitted by law, to ensure that the provider does not do so without the customer's involvement. The customer also will want to require, of course, that the provider immediately investigate the cause of the breach and cooperate with the customer in mitigating damage caused by the breach.

In addition to the panoply of state laws, for health care companies, the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), enacted as part of the American Recovery and Reinvestment Act of 2009,[9] provides new, federal data breach notification obligations that require HIPAA "Covered Entities" to report most security breaches directly to affected individuals.[10] In general, notices provided under these provisions must be sent within 60 days, [11] which may be a short period of time to investigate and mitigate a data breach in the cloud environment, since the data could be stored in one or more other countries.[12] Any contract with a cloud service provider will need to enable a health care company to comply with these requirements.

Another legal obligation a service provider may have is compliance with government requests for disclosure or when served with a subpoena.[13] Most providers will reserve the right to make these kinds of disclosures when requested, but the customer may want to try to negotiate some limitations on that. For example, the customer should require that notice be given to it before such disclosures are made unless the provider is legally prohibited from doing so.

2. **Regulatory Compliance** –

"Regulations grow at the same rate as weeds." – Norman R. Augustine

---

[8] The California security breach notification law, for example, does not require encryption of computerized data, while the Massachusetts law does.

[9] Pub. L. No. 111-5 (2009).

[10] Pub. L. No. 111-5 (2009) at 13402.

[11] *Id.* at 13402(d)(1).

[12] Covered Entities are also required to notify the Secretary of HHS of all data breaches on an annual basis, and must provide notice of any breach of more than 500 records immediately. These notice provisions apply to "unsecured" protected health information (PHI). Under the HITECH Act, the Secretary of HHS will provide guidance to Covered Entities as to the steps necessary to properly render PHI "unusable, unreadable, or indecipherable to unauthorized individuals" within 60 days after the date of enactment of the HITECH Act and will update that guidance on an annual basis. See Pub. L. No. 111-5 (2009) at 13402(h).

[13] For example, the Stored Communications Act, Title II of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508 Section 201, 100 Stat. 1848, codified as amended at 18 U.S.C. Section 2701-2711, requires service providers to disclose the contents of their customers' electronic communications under certain circumstances.

Customers may be subject to regulations whose requirements the customer will need to pass along to its service providers. For companies in the health care space, HIPAA compliance is a particularly significant issue. Most of the early cloud computing service providers are general providers, rather than companies that specialize in handling medical information. The early providers are banking on their size and the attraction of low costs and other benefits to force customers to accept the providers' standard contracts (which will be discussed in more detail later), but health care companies may need their service providers to execute a Business Associate Agreement, which the current group of providers may not be willing to do. Health care companies also need to confirm that cloud service providers can (and do) comply with both the HIPAA Privacy Rule and the HIPAA Security Rule, particularly since they were updated as a result of the HITECH Act.

The U.S. Dept. of Health and Human Services, through the Centers for Medicare and Medicaid Services ("CMS"), has recently begun to step up enforcement of these rules and, notably, in 2008, Providence Health Services became the first entity to be fined for non-compliance with the HIPAA Security Rule.[14] The health provider was fined $100,000 for failing to provide adequate safeguards for PHI on backup media and laptops.

Because Mr. Augustine was correct in his assessment as quoted above, the contract should allocate the cost of the provider's compliance with changes to regulations and new regulations. If a new or modified regulation forces a provider to modify the service solely because of the requirements of the customer, it's reasonable for the cost of those changes to be passed on to the customer (or allocated directly among its affected customers). However, if the change is due to the nature of the service the provider is offering, in general, then the cost of those changes should only be recaptured in the provider's rates, not passed directly to customers. Depending on how a customer's rates are calculated (i.e., are they fixed for some period of time or can the provider change them through some process), this may place the risk of regulatory changes on the supplier or the customer, but it should be negotiated in advance as part of the deal.

3. **Service Level Terms** –

"No plan can prevent a stupid person from doing the wrong thing in the wrong place at the wrong time--but a good plan should keep a concentration from forming." - Charles E. Wilson

What service level commitment is the provider making, and what does the customer need? Cloud computing providers are looking to maximize their economies of scale, which means (a) they want to standardize their offering as much as possible, which could decrease their desire to provide the kind of flexible service companies are used to receiving in-house or from a dedicated provider, and (b) they want to minimize the commitment they have to provide their customers in terms of service levels and service level credits. Does the service level at least match what the customer has been providing on its own if the resource has been in-house or what the customer has been receiving from a third party? In some cases, the customer may need to determine internally what service level it needs if the service is new to the organization. Along these lines,

[14] *See* Providence to Pay First HIPAA Fine of $100,000, http://www.thompson.com/public/newsbrief.jsp?cat=BENEFITS&id=1853 (last visited on Jan. 29, 2009).

the downtime maintenance windows (and notice requirements) reserved by the provider should be considered to ensure they do not conflict with the customer's expected usage of the service.

In addition, what metrics are being used to track the service level commitments? The provider should analyze and determine upfront, when designing the service, the metrics that customers will demand since the provider does not want to be in a position of applying different metrics for different customers.

Additionally, what remedies are provided in the agreement for failure to meet those commitments? Often the provider will limit those remedies to service level credits, usually expressed in terms of a percentage of monthly fees paid, or termination of the agreement if the failure to meet the service levels is severe. Moreover, these credits usually must be requested by the customer, within a certain time period, in order for them to be applied against the customer's account. The customer will want to consider whether it has processes in place to make this request and comply with these procedures, if it cannot negotiate a less strict process.

4. **Ownership of Data** –

"As a man is said to have a right to his property, he may be equally said to have a property in his rights" – James Madison

The agreement should also address who owns the data generated through use of the service and what rights if any the other party would have to it. This includes not only the data input by the customer (which the customer would own), but also data processed by use of the system (which the customer typically would own), as well as "metadata" (the application and network infrastructure information describing the customer's operation and use of the system which the provider would usually own but which the customer might want to be able to use, in order to obtain the service elsewhere, once the relationship is terminated).

5. **Indemnification and Liability** –

"*Everybody wants to take responsibility when you win, but when you fail, all these fingers are pointing*." - Mike Krzyzewski

What liability is the provider willing to take (for example, intellectual property infringement claims as to the service) and what liability does it disclaim? Is the provider's overall liability capped, and if so, does it have any exclusions (such as for infringement or willful misconduct)? The customer should consider whether other liabilities (such as for confidentiality or security breaches) should be excluded from these limitations. From the provider's viewpoint, it may suffer certain liabilities for the customer's use of the service (e.g., uploading infringing materials, spam, etc.). How, if at all, is the customer's liability limited and does this limitation also have appropriate exclusions?

6. **Disaster Recovery & Business Continuity** –

"What do you mean, 'Ooops'?!?" – Bill Cosby

The service agreement should clearly spell out the service provider's responsibility, if any, for customer data back-ups, including the frequency with which back-ups are to be performed. In addition, the customer will want to ensure that the service provider has appropriate disaster recovery and business continuity plans, including redundancy, recovery time objectives and appropriate notification and escalation processes, in place to handle disasters and catastrophic events that cause service outages. Customers should also recognize that a cloud provider can create a single point of failure, as the Carbonite customers learned. Both ends of the internet connection and the cloud service, itself, could cause your data or the service to be inaccessible. Outside of the issues of SLAs and credits, you need to have a plan for dealing with that possibility.

7. **Termination** –

"Don't go away angry, just go away." – Corporal "Stitch" Jones, "Heartbreak Ridge"

Issues relating to termination of the relationship also need to be considered up front. What if the provider goes out of business? Is there a mechanism for the customer to get access to its data? Some technology escrow service providers now offer data back-up services as a protection against service provider failures. The customer should consider whether the use of such services, or other back-up capabilities, is needed. From the provider's perspective, what if customer fails to pay or goes under? What obligations does the provider have to maintain or return data?

From the customer's perspective, the provider should have an obligation to assist with the customer's transition to another supplier regardless of the reason for the termination (i.e., even if the provider is terminating the customer for cause). If the provider is terminating the customer for failure to pay, then it's reasonable for the provider to insist on payment in advance for the transition assistance, but if a provider could terminate the services and effectively shut down a customer's business until the customer can find and bring up the services with another supplier, that puts too much leverage on the provider's side.

8. Cloud Lock-in (and Open Source) –

"*Man is the only kind of varmint sets his own trap, baits it, then steps in it.*" - John Steinbeck

However, there are a couple of additional issues to consider with respect to termination of the relationship. Depending on the level of abstraction of the cloud computing environment, the customer may have difficulty in porting its data and applications used in that environment to a different environment. If it's a low level of abstraction, for example, such as that offered by the Amazon platform, portability is less of an issue than at the higher level of abstraction offered by such cloud providers as SalesForce.com. This difficulty in porting and interoperability, referred to as "cloud lock-in," should be considered by the customer up front when assessing its needs for cloud services, for even if the customer were to obtain some level of transition assistance from the cloud provider, it is not likely to get the provider to agree to re-port the data or application so that the customer can use them with a competitor.

Unlike a traditional software licensor/licensee relationship, the customer does not have the underlying software on which the services were provided. In addition to escrow services for customer data and transition assistance to the customer, some cloud customers may wish to obtain a license to some or all of the software used to provide the cloud computing service, much as they would do in a software license arrangement. The provider may not agree to this for a couple of reasons – first, the platform for its service is built on the software, and the provider would not want release this "secret sauce" (much as a software provider is protective of its source code); second, many cloud computing implementations use open source software,[15] some of which are likely subject to licenses which require that if the software is modified and distributed, the modifications must be made available in source code form. Making the software available even through an escrow arrangement could trigger this obligation, which cloud providers will undoubtedly wish to avoid.

9. **Pricing** –

"Show me the money!" – Jerry Maguire

Like any deal, the pricing structure for cloud services needs to be carefully examined before you sign the deal. Cloud services providers like to sell their services on a "utility" model, emphasizing the ability to "dial-up" or "dial-down" the services to reflect the customer's needs. When it comes to the contract, however, the deal frequently includes minimums that make it much less of a utility model and much more of a "take or pay" with pricing specified for growth. If the specified floors are reasonable, that may not be a bad thing, as the commitment to a minimum level enables the providers to provide certain pricing incentives that would not be available in a pure utility model, but if the last 12 months have taught us anything, it should be that you never know what a business downturn is going to bring.

10. **Early Versions of Contracts and Ongoing Updates** –

"Never allow someone to be your priority while allowing yourself to be their option." – Anon.

Most suppliers are rushing these complex services to market and are developing their contracts in the same "release the beta" model that has become the norm for technology services. Because of that, suppliers are using contract forms that are sometimes incomplete and sometimes internally inconsistent. The service providers are also looking at these contracts more like online terms of service that they can amend and modify at will – including the pricing and SLA provisions. Even if the provider's service agreement is presented to the customer as an online, click-through agreement to which the customer has little choice but accept or find another vendor, the customer is still well-advised to read and understand how key issues are addressed in the agreement, since it may be possible to negotiate certain of these provisions – and if the contract terms prove non-negotiable, that should be a signal to you about how issues in the relationship will be resolved in the future.

[15] Jon Brodkin, Open Source Fuels Growth of Cloud Computing, Software-as-a-Service, Networkworld, July 28, 2008, available at http://www.networkworld.com/news/2008/072808-open-source-cloud-computing.html?page=1

While the recent expression of outrage over Facebook's proposed change to its terms of service implies that those suppliers who unpleasantly surprise their customers may do so at their peril, the prospect of signing up for such a critical service where the contract can be changed by one side should give potential customers pause.

CONCLUSION

"Knowing a great deal is not the same as being smart; intelligence is not information alone but also judgment, the manner in which information is collected and used." - Dr. Carl Sagan

Cloud computing services offer the promise of greatly extending IT resources in this environment of cost-consciousness and resource constraints. However, both the service provider and the customer should ensure that the terms of the service agreement enable both parties to meet their legal obligations and satisfy their business requirements. Customers looking to take advantage of the cloud need to remember that this is a new area and service providers are not experts in **your** business – they haven't thought through all of the issues associated with specific industries or business models. Similarly, companies looking to provide cloud services need to remember that potential customers are not used to thinking about issues raised by the using of the cloud, and helping them think through those issues before you sign a deal will lead to a happier, longer, more successful relationship after you sign the deal, even if it means you have to take a little longer to get the deal done right.