The Cloud: Dream or Nightmare?

By: Evan Pilchik, Esq. and Erik Weinick, Esq.
Otterbourg P.C.

As more and more companies migrate their information technology systems to the Cloud, it is important to examine the true costs and benefits that accompany such fundamental operational shifts. Before taking the leap, companies must be sure that the Cloud will actually provide a pillow soft, dream-like landing, as opposed to becoming the cause of endless technology and operational nightmares.

Prior to delving into the pros and cons of the Cloud, it is helpful to establish a working definition. In general, the Cloud refers to the delivery of computer services and functions to a user via the Internet, usually from an off-site third party provider. This stands in contrast to the more traditional method of delivering those same services from devices owned and operated by the user (or his/her organization) at the user's location. Said differently, it is the outsourcing of information technology ("IT") infrastructure and/or services. However, just as the outsourcing of other business endeavors (such as manufacturing and customer service) comes with benefits and costs, so too does migration to the Cloud.

Organizations have flocked to the Cloud for numerous reasons. The Cloud can *potentially* save an organization significant costs by reducing the expense of hardware, the use of precious on-site real estate, and reducing reliance on in-house IT staff to install, monitor, repair and deploy company-owned hardware, software and services. Additionally, Cloud service providers can often provide a broader range of software at lower costs. They can also provide more comprehensive user support, especially for small organizations, which might not otherwise be able to provide round-the-clock assistance to their users.

However, the reality of the Cloud does not always match its proponents' dreams. First, not all companies actually achieve the cost savings they expect. Second, just as credit card and airline customers grow frustrated speaking with customer service representatives continents away during already stressful phone calls, corporate computer users who find themselves working through late night software issues with an employee of their Cloud services provider who is not as familiar with their company as an in-house IT specialist, can become similarly frustrated. That frustration can result in the loss of valuable productivity from that employee.

Cost Savings from the Cloud are Not Automatic

A recent study should give pause to companies which have not yet moved to the Cloud. Nutanix, a Cloud service provider, and Quocirca, a European research and analysis company, surveyed 400 European information technology leaders. Most startlingly, only seventeen percent (17%) of respondents reported that they had, by migrating to the cloud, turned capital expenditures into ongoing, budget-friendly operating costs. Putting cost-savings aside, only thirty-nine percent (39%) said the Cloud had satisfactorily provided new or additional IT functionality faster than traditional approaches (having in-house, or at least on-site, personnel install and manage software on company-operated, on-site hardware), meaning that in addition to the Cloud migration being unjustified from a balance sheet perspective, the migration could also be viewed as unjustified under an IT benefit-based analysis.

This sentiment has also been echoed by Dell Technologies CEO Michael Dell. According to news reports, during his keynote address at the 2017 Dell EMC World Conference, Dell stated that "many customers have already told us that public cloud is twice as expensive as on premise, especially for a predictable portion of their workloads, which in many cases is roughly 90 percent."

Part of the lack of realization of expected savings may be attributed to the billing structures utilized by Cloud service providers. For this reason, companies entering into Cloud service agreements need to understand the billing structure which will be used by their chosen provider.

For example, a quick Internet search reveals numerous customer complaints about the confusing nature of Amazon Web Services' ("AWS") billing. Darryl Plummer is a vice president at Gartner, Inc., an NYSE listed company which describes itself as the world's leading research and advisory company. According to published remarks made by Mr. Plummer at an October 2017 symposium hosted by Gartner, 95% of Gartner's clients reported that AWS bills were the most confusing part of working with AWS. In response, AWS CEO Andy Jassy stated that this confusion is attributable, in part, to the wide array of services offered by AWS, which introduced over 1,000 new features in 2016. Regardless, Cloud customers may be paying for services they no longer need (and thought they had stopped paying for), simply because they do not recognize the charge for that service on their invoice.

Another reason for a lack of realization of cost savings is that companies are simply replicating their on-premise capabilities in the Cloud, without first analyzing whether or not they actually need that amount of computing power or breadth of applications. If the company does not recognize its on-premises over-capacity when migrating to the Cloud, it will simply be duplicating its prior inflated and unnecessary costs post-migration to the Cloud. This situation is no doubt exacerbated by Cloud vendors who suggest purchasing more capacity than is actually necessary in order to give the customer comfort that it will never fall short.

One method available to Cloud users to avoid purchasing services they do not actually require is to employ a consultant (other than the Cloud provider itself) to assist in the migration. That is the primary service provided by companies such as CloudHealth, Cloudability and RightScale. These firms aim to help companies understand their bills, monitor usage and implement appropriate Cloud programs.

Cloud Migration is a Long-Term Commitment

Companies should not be under the misimpression that they can "try" the Cloud for a short time and then, if dissatisfied, readily return to traditional computing or a different Cloud service provider. Rather, migrating to the Cloud computing is a long-term commitment for several reasons.

First, a great deal of effort is needed to effectuate a migration, effort that is wasted and must be duplicated in reverse if a company wishes to revert to the "ground."

Second, many Cloud providers require customers to enter into long-term agreements that may not be terminated early without material consequences. This makes it imperative for companies to conduct their diligence and select the correct provider (in terms of technical prowess, appropriateness of products and services offered, financial viability of the provider, and legal fit). One way to mitigate risk in this regard is to engage multiple providers, with each hosting a different application or applications, so as to avoid putting all of a company's proverbial eggs in one basket. Companies should also try to avoid the IT equivalent of entering into a long-term automotive lease on a year-end vehicle if they are going to regret not having access to next year's new and improved model, which will be available simply by waiting a short time.

Third, if a company decreases its own on-site, company-run operations in favor of the Cloud, and then changes course, it may take a long time and a great deal of expense to bring the company-based hardware and services back on-line. This is especially true if time has passed, the original technology has become outdated and needs to be replaced, and the real estate and personnel previously deployed for IT have been repurposed or eliminated.

Going to the Cloud is Not a License to Ignore Security

The same cybersecurity considerations which apply "on the ground" also apply in the Cloud, even though the Cloud provider may be able to provide more robust and up to date security than the company could economically provide for itself. For example, the implementation of multi-factor authentication ("MFA") for Cloud access is a must. Without it, if a password that enables access to the Cloud is compromised, so is the data secured in the Cloud. Even with MFA, companies should require the regular changing of passwords, and should implement procedures to ensure that access for former employees is actually disconnected. In addition, companies should segment their employees' access to the system. Employees' access should be restricted to those systems and files which are pertinent to their responsibilities. If all employees have access to the company's entire system, then a compromise of any employee, no matter how low level the employee, may compromise the entire company.

Cloud users also still need to guard against malware, which is software designed to damage, disable or take control of computer systems, contrary to the wishes of the owner or authorized

user. When malware is uploaded from a user's device to Cloud applications, it can compromise data that was seemingly safely tucked away in the Cloud. This is particularly important in light of a report by RightScale which estimated that eighty-two percent (82%) of small businesses will rely completely on Cloud services by the year 2020.

One of the easiest ways to guard against the spread of malware is through employee education. Employees should be educated and regularly reminded of the many nefarious ways cyber criminals attempt to infiltrate using malware, such as seemingly legitimate email with dangerous attachments and/or links to "dummy" websites, which, at a quick glance, are identical to the genuine article the user is familiar with and trusts.

Cloud Migration Does Not Alleviate Privacy and Cybersecurity Legal Obligations

Many organizations mistakenly believe that by outsourcing their IT functions to a third party, such as a Cloud provider, they are also outsourcing their responsibility for security, as well as their attendant privacy and cyber security legal obligations and liability. This is simply not the case.

As a threshold matter, most Cloud service agreements expressly disclaim that the provider is taking on such risks, responsibilities and/or liabilities. For example, the publicly available user services agreement utilized by AWS clearly places the ultimate onus for privacy and security compliance on the client, not on Amazon. While AWS says that it "will implement reasonable and appropriate measures designed to help you secure your Content against accidental or unlawful loss, access or disclosure . . . you are responsible for all activities that occur under your account, regardless of whether the activities are authorized by you or undertaken by you, your employees or a third party (including your contractors, agents or End Users.)" AWS User Services Agreement at Sections 3.1 and 4.1(a), found at https://aws.amazon.com/agreement/.

Speaking of contracts, Cloud users should understand what their service agreement does and does not provide for. For example, before migrating to the Cloud, a company should analyze whether the service agreement:

- Requires the provider to encrypt data
- Restricts the access of the provider's own employees to the company's data
- Grants the user a right to audit security procedures and data centers, as well as the right to be promptly notified of breaches or other issues
- Details how data is handled in the event that the provider's business fails
- Contains provisions (either from a legal and/or technical perspective) to recover or recreate data that is held by the provider
- Requires the provider to return the data to you, or escrow it with a third party before going out of business
- Makes clear that, in the event of a sale of the provider, or its bankruptcy, that the provider may not sell or transfer your data without your authority
- Contains clear statements regarding the provider's level of security and data protection precautions

Other important legal considerations include making sure that the company's Cloud-based data is accessible in the event of litigation. Companies need to make sure that, even after migrating to the Cloud, they can fulfill their obligations to institute litigation holds (suspension of data destruction procedures when litigation is foreseen) or to respond to subpoenas. Moreover, companies need to make sure that their Cloud provider can provide timely access to the relevant data, and in a useable form.

Another critical consideration for a company contemplating a move to the Cloud is what law applies to the relationship. Companies need to analyze this in advance, lest they find themselves non-compliant with the laws or regulations of a jurisdiction to which their only relationship is that their Cloud provider has located servers in the jurisdiction. Given that context, a company must understand where its data will actually be stored, how the vendor will respond to subpoenas for the company's data by that jurisdiction's officials, and what protocols the provider has to insure compliance with the regulations that apply to the company.

All companies which receive, store and transfer data must understand that transferring that data across borders may trigger additional legal obligations (or actually violate legal obligations). This problem is amplified by the use of the Cloud, where data may flow across borders without the company's affirmative action implementing such a transfer. For example, while a company may recognize the restrictions it faces in sending personally identifiable information from one of its servers in the European Union to the United States, it may not be aware that data it transfers to a Cloud provider in the European Union may

wind up backed up on a server outside of the European Union, which may potentially run afoul of such regulations as the European Union's General Data Protection Regulation, or GDPR.

Another jurisdictional consideration is the requisite standard for the safety and security of data. These standards vary by jurisdiction (such as country by country, state by state, or even industry by industry), and as discussed above, a company is ultimately responsible for meeting these standards, even if a Cloud provider or other outsourcing firm is largely running the company's information technology functions.

Finally, companies should understand how their use of the Cloud interacts with their cyber insurance policy. The definitions of terms such as "computer system" or "computer network" in a cyber insurance policy could mean that Cloud computing is not covered. Companies should therefore ensure that there are no exclusions for use of the Cloud, or for particular Cloud providers that will leave them without the insurance coverage they expect in the event of a cyber incident.

Conclusion

As should be clear from the foregoing, while the Cloud may have significant advantages for companies of all sizes, those considering a migration must do so fully cognizant of the risks and rewards.

About the Authors:

Both of the authors are certified as Information Privacy Professionals (CIPP-US) by the International Association of Privacy Professionals (IAPP) and co-founders of the Privacy & Cybersecurity practice group at Otterbourg P.C., which counsels firm clients on privacy and cybersecurity matters.

***Evan Pilchik** is also a member of the firm's corporate restructure and finance departments and represents banks and other financial institutions in structuring, negotiating and documenting a diverse array of financing transactions and workouts.*

***Erik Weinick** is also a member of the firm's litigation practice group and regularly represents a diverse group of clients (including many commercial and specialty lenders) before state and federal courts, regulatory authorities, and alternative dispute resolution tribunals.*