US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Common Risks of Using Business Apps in the Cloud

Sandy Shrum and Paul Murray

Businesses Are Using Cloud Apps

What is the *cloud*? In general, the cloud is the concept of remotely hosted IT services, termed *cloud apps*, provided by a supplier. These suppliers are called *cloud providers*. Typical cloud apps offered by cloud providers include email, calendar, documents, online storage, sales, customer service, and more. Some of today's many cloud providers are well-known names in industry and include companies such as Amazon, Google, 37signals, Intuit, Microsoft, and Box. A selection of the top cloud apps in the market today include Cloud Drive, Google Apps for Business, Skype, SalesForce, Basecamp, Quickbase, and Box Business.

Using business apps in the cloud has widely recognized advantages: you save money by paying for only the IT computing resources you need, you can ramp up (or ramp down) computing resources quickly without capital investment, and you can increase your reach to employees and users anywhere on the planet.

This paper will (1) describe the risks you should understand and look for when partnering with cloud providers and (2) describe actions you can take to mitigate these risks.

Common Risks of the Cloud

You don't have total control. When you purchase IT services from a cloud provider, you don't have complete control over the computing resources your business needs to operate. What happens if the cloud provider goes out of business or changes its services or prices? What if it has an outage? In December 2012, Netflix and many of its customers experienced a total outage for two days—Christmas Eve and Christmas Day—because their cloud provider, Amazon, had a service outage to the Eastern United States.

In the *Bloomberg Businessweek* article, *The Cloud Carries Risk*, Verne Kopytoff writes, "A recent study by the International Working Group on Cloud Computing Resiliency, made up of academic and technology industry representatives, tried to quantify the cost of outages. It

estimated the combined downtime at 13 major cloud service providers to be 568 hours since 2007—with an economic impact on customers of at least $71.7 million."[1]

You might get stuck with one supplier. Not all cloud providers are the same. Their platforms are different with different hardware, software, configurations, and settings. Therefore, abruptly changing from one supplier to another can be difficult, even if you use the same app. You might get stuck with one supplier, just as you might with internally deployed apps. Email is a great example. The migration of email from one vendor to another is likely to encounter problems with the conversion of mail formats and customizations, whether on the cloud or in house.

An app, especially a customized one, may not behave the same or even work properly on another cloud. If you begin to have problems with a cloud provider, it can be a long process to disengage and begin a new relationship with another provider. Until there is more standardization across the cloud-provider industry, switching from one provider to another will be a complex endeavor.

Your data is protected by someone else. When using a cloud provider, your data typically is housed and protected by the cloud provider. Although the provider may be more able to purchase the latest security software and support, it doesn't have the same motivation to protect your data as you do. Granted, their business is reliant on their ability to protect data, but do they run their business like you do?

The risks to data expand beyond data being destroyed. Trade secrets can be lost or data may be frozen because of a subpoena or other government action. Trade secrets can be stolen when a malicious actor takes the encryption keys needed to access your data. Let's say the cloud provider advertises that it provides encryption and encrypted backup services to protect your cloud data. On the surface, that seems fine, but these services may not be sufficient for every business. Many providers use common encryption keys they control for both storage and backup of customer data, which means that the malicious actor must only infiltrate the cloud provider to gain access to the data.

An example of frozen data due to government action is the case of Megaupload, a cloud file storage and viewing service. Charges against individuals at Megaupload resulted in law enforcement seizing over $50 million of Megaupload's assets. This seizure meant that its customers, who had data on Megaupload's servers, could not access the data even though they had done nothing wrong.

To complicate matters, your cloud provider is likely to be located far from your business physically. It is probably located across state lines or even in other (and multiple) countries. The locations of these data centers have legal implications. If your data is involved in a criminal case, the laws of the country and state where the data center is located dictate what the government can control. Your business data could be taken hostage even though you are not at fault. Further, many countries have stricter laws than the U.S. when it comes to encryption. A country may not allow data to enter or exit the country if it is encrypted using certain encryption techniques.

---

[1] Kopytoff, Verne. The Cloud Carries Risks, Too. Bloomberg Businessweek, August 2012. http://www.businessweek.com/articles/2012-08-07/the-cloud-carries-risks-too

Therefore, performance benefits of internationally available data may require a tradeoff of lesser encryption to not violate laws in the country where the data center resides.

Your security is managed by someone else. Cloud providers are by design very large consolidators and aggregators of information in comparison to a typical corporate data center. In general, cloud providers have platforms that are more secure than your own or at least as good as yours because they have more resources than most (especially small) organizations to devote to security.

However, since cloud providers house multiple customers' data on the same servers and they manage a much higher volume of data than even large organizations, they have the potential of being more desirable targets for cyber criminals. So even if we haven't seen large attacks in the cloud much today, historically we have seen large companies with large security resources attacked. Those large businesses understood their business needs and were tuned to their own business model. Can a cloud provider's security be tuned to every business model and workflow of all its customers?

You have to fight for information. Believe it or not, some of the largest cloud providers do not allow their customers to conduct inspections. Some cloud providers supply their customers with audit results such as a 3rd party SAS 70 type I and type II audits (or its replacement the SSAE 16) and various others. However, not all audits are equal.

Risk Mitigation in the Cloud

Know what's already going on. Be sure you know what staff members in your organization are doing. Are they taking action without asking permission? For example, a project team may assume that it can use a cloud provider to quickly work on a proof of concept for a new tool. Or maybe the marketing department decides to purchase CRM services from a cloud provider instead of waiting months for a homegrown service. Staff can purchase these services easily by using a credit card or getting a free trial, unaware of the risks they are taking.

Be a smart consumer. Select suppliers who are willing to enter into agreements that enable you to operate your business effectively. In particular, make sure that the cloud provider's security controls are tuned to your business needs sufficiently. You may have an opportunity to negotiate a service level agreement (SLA) with a cloud provider, but more likely you will need to compare the SLAs of different providers and find the one that best defines the terms you need.

Almost all cloud-provider SLAs have indemnification clauses that try to eliminate or isolate the cloud provider from responsibility or risk from loss to a business due to a service outage. Even if the terms limit risk and responsibility, it is in your best interest to negotiate those terms. If you do not have a contracts attorney on staff, a good time to find one is *before* signing with a cloud provider. You may not gain significant ground, but it is essential that you understand the terms and risks with each cloud provider to make an informed decision.

If you can, negotiate contract terms that define your requirements for the computing resources, including security, data handling, and disaster recovery. Pay particular attention to your rights and obligations related to being notified of breaches in security, data transfers, creation of derivative works, change of control, and access to data by law enforcement. Also make sure you

understand where your data will physically be located and the laws that pertain to those locations, including who is considered to own the data.

Involve the right people in cloud decisions. Supplier selection, monitoring, and management are skills you must have to manage suppliers critical to your business. Find experts in your organization that understand supply-chain management. Involve both business leaders and IT professionals in making the decision about which cloud provider to select. As a business investigating a prospective cloud provider, it is critical that you read available audits and assess the reputation of the auditor as well.

Be cautious. Build trust with cloud providers slowly. Start by using the cloud provider for non-critical services and evaluate how well they meet your needs and avoid problems. Slowly build trust over time by extending what you use on the cloud little by little. Using this incremental approach buys time and opportunity to learn and make adjustments to the business relationship.

Be selective about what you control and what you choose to be supported on the cloud. Keep your business-critical apps off the cloud, at least at first. If you can maintain control over data from the app, maintain that control. Compare the risks and benefits of keeping your apps and data on your systems vs. the risks and benefits of moving it to the cloud. Both choices have risks; consider them all to make a good decision. Select providers that have a mechanism for unique encryption keys per customer. This mechanism is intended to reduce the risk of unauthorized access to your data. Instead of being controlled by the cloud provider, these keys can be controlled by you or securely escrowed to ensure recoverability.

Monitor your cloud provider's activities. Find a way to ensure that the terms of the SLA are being honored. Keep abreast of the security controls used by the cloud provider and its ability to keep up with trends in cyber crime. Demand the information you need to monitor your business on the cloud. You should have access to the same information you would if the service was in your organization. Include terms in the SLA that ensure you have the right to receive the information you need without resistance. Be as specific as possible to protect your access to critical information.

Plan for cloud outages. All cloud providers have outages. Amazon, Salesforce, and Microsoft are only three of the cloud providers that had outages in the last year. Ask the cloud provider about its disaster recovery plans and have a disaster recovery plan of your own that includes cloud apps.

Investigate a hybrid approach in which you have a private cloud that works with a public cloud. You, or a paid cloud management service, manage your private cloud to scale to a public cloud as capacity is needed. Also consider a multi-public cloud implementation of a service across two or more cloud providers. Doug Dinely of InfoWorld writes, "VMware, Microsoft, and open source rivals OpenStack and CloudStack are building cloud software stacks designed for both private and public deployments, giving administrators common management tools, and developers common APIs, across the different environments. Similarly, Eucalyptus has built its private cloud business on compatibility with Amazon Web Services APIs, allowing customers

who have built applications on AWS to deploy them on-premise, and vice versa."[2] These solutions are short of a seamless jump from any provider to any provider, yet they enable you to build a cloud solution that mitigates the risk of outage.

Conclusion

You can use cloud apps for your business; just be sure to fully understand the risks and how they might affect your particular business and industry. Be aware of how your staff may already be using the cloud, be a smart consumer of cloud services, involve people with the right skills in making cloud decisions, use an incremental approach to build trust slowly, monitor your cloud provider's activities, and plan for cloud outages. These activities will help you benefit from cloud service flexibility and cost savings while protecting your business.

Further Reading

1. Babcock, Charles. "6 Reasons to Use Multiple Cloud Providers," InformationWeek, March 2012. http://www.informationweek.com/cloud-computing/infrastructure/6-reasons-to-use-multiple-cloud-provider/232800011 (accessed January 22, 2013).

2. Burns, Christine. "10 Cloud Predictions for 2013" ComputerWorldUK, December 2012. http://www.computerworlduk.com/slideshow/cloud-computing/3414733/10-cloud-predictions-for-2013/ (accessed January 22, 2013).

3. CyberMedia Research. "The Cloud and the Law: An Interpretation of Key Contract Clauses for Late Adopters Like the Healthcare Sector." June 2011. Available: http://cmrindia.com/the-cloud-and-the-law-an-interpretation-of-key-contract-clauses-for-late-adopters-like-the-healthcare-sector/ (accessed January 16, 2013).

4. Dineley, Doug. "Hybrid Cloud: Extend Your Private Cloud with Public Cloud Services." InfoWorld, April 17, 2012. http://www.infoworld.com/t/cloud-computing/hybrid-cloud-191074 (accessed January 22, 2013).

5. Electronic Privacy Information Center. "Cryptography and Liberty 1999: An International Survey of Encryption Policy, 1999." Available: http://www.gilc.org/crypto/crypto-survey-99.html (accessed January 16, 2013).

6. Hon, Kuan. "Data Protection, the Law, and You." Computerworld UK, April, 2011. Available: http://blogs.computerworlduk.com/cloud-vision/2011/04/data-protection-the-law-and-you-1/index.htm (accessed January 16, 2013).

7. Kopytoff, Verne. "The Cloud Carries Risks, Too." Bloomberg Businessweek, August 2012. Available: http://www.businessweek.com/articles/2012-08-07/the-cloud-carries-risks-too (accessed January 15, 2013).

---

[2] Dineley, Doug. "Hybrid Cloud: Extend Your Private Cloud with Public Cloud Services." InfoWorld, April 17, 2012. http://www.infoworld.com/t/cloud-computing/hybrid-cloud-191074

8. Mell, Peter and Grance, Timothy. “The NIST Definition of Cloud Computing.” NIST Special Publication 800-145, September 2011. Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (accessed January 15, 2013).

9. Patel, Ash. “Cloud Computing Providers—An Attractive Target for AET-based Attacks?” Secure Business Intelligence, May 2012. Available: http://www.scmagazineuk.com/cloud-computing-providers--an-attractive-target-for-aet-based-attacks/article/243331/ (accessed January 16, 2013).

10. Rana, Sadhana & Joshi, Pramod Kumar. “Risk Analysis in Web Application by Using Cloud Computing,” Zenith International Journal of Multidiciplinary Research, Vol 2, Issue 1, January 2012. Available: http://zenithresearch.org.in/images/stories/pdf/2012/Jan/ZIJMR/30%20SADHANA%20RANA%20AND%20PRAMOD%20risk_analysis_in_WebApplications_by-Cloud_Computing.pdf (accessed January 15, 2013).

11. SAS70.com. “Service Auditors Reports.” Available: http://sas70.com/sas70_reports.html (accessed January 16, 2013).

12. Soghoian, Christopher. “Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era.” Journal on Telecommunications and High Technology Law, pp. 359-424, Issue 1, 2010. Available: http://heinonline.org/HOL/Page?handle=hein.journals/jtelhtel8&div=18&g_sent=1&collection=journals (accessed January 16, 2013).

13. Spinola, Maria. “An Essential Guide to Possibilities and Risks of Cloud Computing.” January 2008. Available: http://www.mariaspinola.com/whitepapers/An_Essential_Guide_to_Possibilities_and_Risks_of_Cloud_Computing-A_Pragmatic_Effective_and_Hype_Free_Approach_For_Strategic_Enterprise_Decision_Making.pdf (accessed January 15, 2013).

14. Weiss, Todd R. “Cloud Fail: The Real Risk of Cloud Computing in Your Business Is Not Involving Your IT Team.” June 2012. Available: http://h30565.www3.hp.com/t5/Clearing-Up-The-Cloud/Cloud-Fail-The-Real-Risk-of-Cloud-Computing-in-Your-Business-Is/ba-p/4548 (accessed January 15, 2013).

15. Yoran, Elad. “Encryption of Data-in-Use to Harness the Power of the Cloud.” Cloud Computing Journal, November 19, 2012. Available: http://cloudcomputing.sys-con.com/node/2449343 (accessed January 16, 2013).