SRG Security Services Technology Report
Cloud Computing and Drop Box
April 2013
Cloud Computing in the Industry

Introduction to Cloud Computing

The term cloud computing is simply the use of computing resources delivered over a network (typically the Internet). Cloud computing is a new way of delivering hardware and software computing resources but it is not necessarily a new technology. When data or photos are stored online (Google, Dropbox, Evernote, etc.) a cloud computing service is being used.

The use of cloud computing comes from a strong focus for business to offset hardware, software, support, and subject matter expertise (SME) costs to a third party. This allows a business to reallocate IT operating costs within the unit or business to meet other goals. One drawback as seen by the industry is that business and personal data is stored within the cloud provider’s facilities. This could lead to unauthorized access or disclosure of the data.

Common Cloud Services

Cloud computing and cloud services are very generic terms and many times the meaning and functionality is misconstrued. Some of the common services that can be provided through the cloud include:

*Infrastructure as a Service (IaaS)*

In the IaaS model, a cloud provider provides physical and virtual machines and other resources (firewalls, load balancers, intrusion detection systems, hypervisors, KVM, etc.) for the customer to use. The customer may or may not administer the provided infrastructure resources.

*Platform as a Service*

In the PaaS model, cloud providers deliver a computing platform typically including operating system, programming language execution environment, database, and web server. Developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the layers of infrastructure required.

*Software as a Service*

In the SaaS model, cloud providers install and operate application software in the cloud and users access the software from cloud clients (typically a web browser). The cloud users do not manage the cloud infrastructure and platform on which the application is running eliminating the need to host and support their own infrastructure.

*Network as a Service*

A type of cloud service where the capability provided to the user of the cloud service is to use network connectivity services. Traditional NaaS services include flexible and extended VPN and bandwidth on demand.
Benefits of Cloud Computing

There are many reasons why business finds the concept of cloud computing enticing and it comes down to being able to do more with less. Since cloud computing is essentially a form of outsourcing, they will have some of the key benefits in common:

- Increase productivity with fewer staff.
- Reduced and variable spending on infrastructure instead of longer term commitments.
- Globalize a workforce cheaper and quicker than the business could.
- Reduced capital costs by spending less on hardware, software, licensing, etc.
- Improve accessibility to applications and data.
- Less personnel training and access to subject matter expertise without the investment.
- Improved flexibility and a quicker response as industry changes.
- Less tie to specific brands as one-off solutions are more easily achieved.
- Can simplify a “bring your own device strategy” by having less importance on the client platform.
- Can offset risk to the provider.

Concerns with Cloud Computing

Data Security and Integrity

Since Internet services have proven to be difficult to protect, one of the primary concerns with cloud computing is security. Large companies hosting massive databases of corporations information is extremely attractive. Organization must understand their information and apply safeguards that are appropriate to its sensitivity in order to protect it. Tools and processes such as a Privacy Impact Assessment (PIA) and/or a Threat Risk Assessment (TRA) are valuable to make safeguard assessments. In order to protect information, organizations using cloud services should:

- Limit access to information and ensure it can only be accesses by those that need to.
- When possible, ensure data is segregated from other client data.
- Ensure strong or multi-factor authentication mechanisms are available.
- Understand any encryption mechanisms used by a provider.
- Ensure response procedures are in place in the event of a data breach or security incident.
- Ensure the provider has a plan and procedure to cope with a disaster and to continue business.
- Ensure periodic audits are performed against the provider and review results when possible.
- Ensure contracts are developed in a manner that protect information and prevent the provider from accessing or disclosing it.
- Have an exit strategy to repatriate or move information to another provider.

Information Privacy Concerns

Within Canada, it seems to be perceived that using non-Canadian cloud services is against the law. This is not the case but there is legislation in place that affects private and public organizations differently. The laws vary between provinces as well.
The privacy concern started when the United States passed the USA Patriot Act which expanded the powers of law enforcement and national security agencies to carry out investigations and to obtain intelligence in connection with anti-terrorism investigations. Canadian public sector unions feared that government and private personal information, including health information, if hosted in the USA would be readily available to US authorities. Today this concern still exists but it’s starting to decline. Regardless of where the information resides, it will always be subject to lawful disclosure to law enforcement or national bodies.

There is no law that prevents most Canadian businesses from “exporting” personal information. Private sector privacy laws require that you ensure a comparable level of security for personal information, regardless of whether you permit it to be managed by a Canadian company or a non-Canadian company. Some highly regulated industries, such as banking, have special rules which may include additional regulation for outsourced services.

As for public sector or government, only British Columbia and Nova Scotia have laws strictly regulating the export of personal information from Canada by public bodies. For all other jurisdictions, including the federal jurisdiction, export is permitted but the public body must ensure a comparable level of security for personal information, regardless of whether you permit it to be managed by a Canadian company or a non-Canadian company.

Alberta has enacted legislation that makes it an offense for a public body or a service provider to disclose personal information in response to an order that does not have jurisdiction in Alberta.

**Public Cloud Services**

When using cloud services one needs to remember that they have less control over changes made to the environment. This is especially true for public cloud services such as Dropbox, Evernote, etc. In 2011 Dropbox accidentally removed all password protection from its users’ files for nearly four hours. And just recently Evernote users were notified of a potential security breach and has instructed all of its users to change their passwords.

Again, it goes back to understanding one’s data and information. If an organization wants to use a service such as Dropbox to share files will an external party to design their public website, the precautions would likely need to be low. If the data is internally confidential and remote users need access, a Dropbox solution might not be the best option.

**End Point security**

Another point to consider with cloud computing is to ensure the end-to-end security of a service. It does no good to have an extremely secure cloud service that is accessed from a client device (such as a tablet computer) that does not enforce a passcode lock, is not encrypted, and has saved passwords to access the service.
It is extremely important to understand the security measures within a cloud service, especially public services such as Dropbox and Evernote. There are even cloud services that can scour other public cloud services, that when provided access to by a user can give a single view of all cloud services. Now the security of that service needs to be verified.

Cloud Computing in the Industry

Gartner predicts that cloud computing will continue to grow, mature, and become an integral part of Information Technology. Many organizations will leverage external services for cloud based projects but it is less likely that they will use external providers exclusively to manage all aspects of cloud services.

Lately there has been demand for a new IT service provider role that the industry is calling cloud services brokerage (CSB). The IT provider functions as the liaison between the cloud service provider and the client organization. This role can ease the burden for companies that are resource strapped to pursue cloud computing services on their own.

Dropbox

Dropbox is one of the most popular cloud based file-sharing services available on the Internet. Dropbox reached the 100 million-user milestone in 2012 and the users are mainly on the consumer side. Dropbox has not been widely adopted on the enterprise side. This can be attributed to Dropbox historically focusing on developing a consumer product, but their focus has changed with the rebranding of Dropbox for Teams to Dropbox for Business in early 2013. Dropbox is trying to position itself as a business tool to compete with other services that have already been enterprise focused, such as Box.net. Dropbox does claim that 95% of Fortune 500 companies and two million small businesses have at least three active users licensed.

IT departments have historically feared the use of these file-sharing services due security concerns and lack of control over corporate information. Some of the changes to Dropbox that IT departments would like to see include:

- Having control over encryption keys.
- Improving corporate directory integration.
- Having the ability to recover employee data if they leave the company.
- Including a policy enforcement mechanism.
- Having the option for an on-premises version (which Dropbox has no plans for).
- Bulk provisioning of accounts.

DropBox for Business tries to meet some of these concerns by introducing new features such as:

- Single sign-on functionality that can be tied into Active Directory for quicker user deployment and management.
- Two-factor authentication.
- Security and password based policies.
Along with the new features Dropbox maintains a strong focus on security mechanisms such as:
- Encrypted file stores on Dropbox using AES-256 standard.
- Uses the SSL secure tunnel protocol (AES-256) while data is in transit.
- Dropbox data is designed to achieve high integrity and availability by using the Amazon S3 service with multiple data centre replication.
- Two-step verification is on option to increase security (recommended).
- Third party apps can add an additional layer of encryption to data.
- User management (add/remove as team changes).
- Business administer dashboard to display usage.
- Events reporting.
- Remote device unlinking.
- Deletion recovery (undo changes).

**Risks/Cautions**

Dropbox, like all Internet services, are susceptible to attack and hacking. In 2011 Dropbox disclosed that all of its users’ files were publicly accessible for nearly four hours due to a bug in an authentication mechanism. Anyone could access a Dropbox account without using the correct password. Another security hole was discovered in Dropbox’s iOS app, which allowed anyone with physical access to the device to copy the login credentials — because it stored user login information in unencrypted text files.

There are also many third-party apps that can also connect to DropBox to access the file store. An organization needs to be aware of the security risks of those applications as well that have direct access to Dropbox data. Users may have the ability to install and use these applications on personal and/or corporate tablets and devices.

Dropbox has a web version, a desktop version, and tablet versions and restricting or preventing employees from using these services may be difficult for an enterprise to enforce which can result in data leakage that the enterprise does not know about.

Another area of concern for some organizations is the location of where data is being stored (geographically) and due to the fact that the enterprise loses control of the data. For these reasons the Government of Saskatchewan has specific requirements when using cloud based services and have had a specific app developed to meet their needs.

**Mitigations**

If an organization is going to use Dropbox, some of the following items may help to mitigate some risk:
- Assume the service is public and only store data that is not sensitive.
- Encrypt files prior to storing on Dropbox. The increases complexity as it will involve using an encryption solution.
- Strong end-user security/risk education on using the service.
- Use-two factor authentication.
- Unlink devices that are no longer in use.
Enable email notifications for account changes.
Manage any linked applications.
Use strong passwords.
Change passwords frequently.

Alternatives

There are enterprise alternatives to using Dropbox, but they are not nearly as popular and most likely not as convenient; Syncplicity (acquired by EMC), Cubby, Huddle, Egnyte, ShareFile, etc. These alternatives have been listed just as information and have not been listed in any particular order.

One company that is rapidly growing in popularity is called WatchDox. They have a Dropbox-like product, with security of the utmost importance, which is aimed towards enterprises. They provide both cloud and on-premise solutions, but the on-premise solution allows the enterprise to maintain full control of the information that is being shared or collaborated on. On-premise is a great alternative to eliminate nerves associated with storing data in the cloud.

Conclusion

Cloud computing is a broad topic with various issues and many variations regarding the scope of deployment. Organizations must take care to fully assess the benefits, risks, and implications of security and privacy when considering a cloud computing solution. They must fully understand their data and its sensitivity in order to make an informed decision on how it needs to be protected.