MAKING THE LEAP TO THE CLOUD: IS MY DATA PRIVATE AND SECURE?

TAX & ACCOUNTING

THOMSON REUTERS

MAKING THE LEAP TO THE CLOUD: IS MY DATA PRIVATE AND SECURE?

Cloud computing: What's in it for me?

The more you know about cloud computing, the more you'll understand why it has received so much attention in recent years. Also referred to as hosted computing, cloud computing generally refers to a complete software solution that your firm accesses over the web. It uses a centralized data center, which is a facility used to house computer systems and associated components, such as telecommunications and data storage systems. Cloud computing provides secure anytime-anywhere access, high-level security and data privacy, and it holds the potential to bring about some of the most far-reaching efficiency and productivity improvements ever seen in the tax and accounting profession. Its benefits include:

- **Reduced costs**–Firms pay incrementally for cloud computing software, saving firms money and making budgeting easier and more predictable.
- **Safer data**–Cloud computing offers an unprecedented level of physical protection against fire, flood, data theft, and other concerns.
- **Anytime/anywhere data access**–You can access hosted data from anywhere, anytime. You can also choose to give your employees any level of access you choose, from full 24/7 access to total lockout.
- **Increased storage capacity**–You can store more data than on firm hosted servers, and storage capacity is easy to upgrade when needed.
- **Worry-free maintenance**–Hardware, software, and security upgrades are handled automatically by professional data center staff. You will always have the latest and most secure technology, with no additional cost or downtime.

Yet, for all its advantages, cloud computing still makes some firms a little uncomfortable, simply because it requires us to think about our data in a different way. How do we know our data is safe when we can't see it? Can we trust a third party with such important information?

The goal of this whitepaper is to address those concerns and clarify complexities around the security and privacy of cloud computing solutions. It outlines cloud computing providers and their role in maintaining the privacy of your client data. And perhaps most importantly, it offers on-the-ground tips that can help you find the right cloud computing provider.

Is cloud computing secure?

If done correctly, yes. In fact, cloud computing offers a level of physical and electronic security that an on-site server or a locked file cabinet can't begin to approach.

Because they can operate with large economies of scale, data centers can be surprisingly affordable, offering even smaller accounting firms a level of security far beyond what they could achieve on their own. But all data centers are not created equal, so it's important to be sure that the one you choose can adequately protect your data. The data center you choose should offer the following protection measures:

Physical Security

- **Redundant power supplies**–Cloud computing data centers have backup power supplies to run servers in case of power outages. In most cases, backup power is provided by diesel generators that can come online instantaneously in the event of a power failure and power the data center for as long as necessary until electricity is restored.
- **Redundant Internet connections**–Cloud computing data centers have several Internet connections that run simultaneously. If one Internet provider fails or is performing poorly, they are able to use other providers that have different Internet backbone services.
- **Redundant hardware**–Tier 4 data centers use multiple hard drives and other components, arranged in such a way that if one fails, another can immediately and seamlessly take its place.
- **Fire and flood**–The data at most data centers is replicated in multiple locations. In the case of a fire, flood, or other disaster, your applications and data can be easily accessed by another computer in another location.
- **Theft**–Data center servers are not easily accessible. Only authorized agents have access to them, and their identity is verified using biometric measures like fingerprints and retina scans. In addition, the entire data center is monitored by surveillance cameras at all times.

Application Security

Application security covers the software side of the data center. It deals with online security issues like hackers and viruses. Application security measures include:

- **Firewalls**–Firewalls act as an electronic barrier between the data center and the Internet. They limit the execution of files and access to data to ensure that hackers and other unauthorized parties cannot access data.

Application Security, continued

- **Anti-virus detection software**–Constantly updated, anti-virus software detects and removes any viruses that penetrate the data center environment.
- **Data encryption software**–This software encrypts data as it travels between your firm and the data center.
- **Administrative controls**–Data centers use administrative controls to govern access to applications and data. They limit access to certain functions and protect client files.
- **Security audits**–Cloud computing providers conduct regular third-party intrusion detection audits. This means they actually hire professional hackers to try to hack into their applications and provide audit reports with their findings. These audit reports highlight any security holes in the applications and infrastructure, which can then be dealt with by data center technicians.

What's my role in cloud computing security?

As we've seen above, most cloud computing providers take extraordinary measures to keep your data safe on their end. But the fact is, the biggest risk to your data comes from inside the firm, from mis-routed data and other simple mistakes to outright data theft by employees.

Cloud computing offers much better protection from internal data loss than other communication methods because it gives you centralized control over your data. It's much easier to establish and enforce policies for a cloud-based system than for the patchwork of email accounts, physical media, and thumb drives that usually results from on-site data storage. However, you are still responsible for establishing and implementing those policies effectively.

The tools you can use to manage access to data include:

- **Administration modules**–Most applications have an administration module that allows a system administrator in your firm to grant user access rights and place restrictions on who can access which files and functions.
- **Firm usage policies**–Firm usage policies are one of the most important tools you have for protecting your data. Can your employees access your systems in public locations where observers can view client data? Can client data be exported to unsecure media and distributed? Can client data be emailed or transferred via unsecure methods?

Your cloud computing provider can work with you to establish good firm user policies. But ultimately, it's up to you to make sure they're communicated to employees and enforced.

Working with your cloud computing provider

Trusting an outside company with something as important as your data can be a difficult adjustment for some firms. But if you choose your hosting company carefully and approach implementation with the right knowledge and expectations, the process can be surprisingly painless.

It's a good idea to look at your relationship with your cloud computing provider as an ongoing partnership rather than a vendor-customer relationship. Considering them an extension of your business will open the lines of communication and help you build a relationship that's mutually rewarding.

The most important thing to remember when you're working with your cloud computing provider is that **you own your data**. The provider should manage the infrastructure and application availability, but they should not have access to your data without your permission.

Here's a quick guide to the ins and outs of managing data between you and your provider:

Note: Although we are highlighting these data privacy concerns in this white paper, these concerns are not isolated to cloud computing providers as they can be issues in protecting data within your own firm.

- **Your cloud computing provider may need to access your data**. They should have policies in place to ask for your permission to access your data when support is needed.
- **You should not assume that support personnel can access your files at will**. Remember, you have the right to deny support personnel access to your data.
- **Most cloud computing providers have data logs in place**. So there is a record of who has accessed your data and when that access took place.
- **It is important to read the privacy statements in your cloud computing provider contract agreements**. These statements will outline how they maintain privacy of your data and what measures can be taken if it is violated.
- **You should ensure that your provider will not use your data for marketing or promotional activities.** In such cases, you should have the ability to opt in to such marketing communications.
- **Remember, it's your data**, and you are ultimately responsible for your clients' privacy.

Questions and Answers

Not all cloud computing providers are created equal. The list of questions below should help you evaluate different providers as you look for the company that can best meet your needs.

How many years have you been providing cloud computing solutions?
Look for a provider that has demonstrated years of experience in cloud computing solutions. Cloud computing has been around for more than 10 years, and the most experienced vendors have worked through all its complexities.

What class of data center do you use?
Look for providers that offer Tier 4 data centers. Tier 4 data centers offer built-in redundancies that are important for protecting sensitive accounting data.

Do you have backup data centers? Is my data replicated at multiple data centers?
Providers with backup data centers can ensure uninterrupted service in case of infrastructure failure. This will also demonstrate the level of investment the provider has dedicated to your cloud computing solution.

What types of security audits do you perform on your systems to protect me from hackers?
Look for providers that contract with third party intrusion detection audits. This demonstrates an ongoing commitment to maintaining the highest level of security.

What policies do you have in place to protect the privacy of my data?
Make sure the provider's employees understand how to protect your data. Ensure that they have procedures in place to maintain their standards.

Have you ever had a security breach? When and how will you notify me if there is a security breach?
Hopefully, your provider has never had a security breach. If they have, find out what they learned from it and how they plan to prevent it from happening again. Also, make sure they have procedures in place to notify you if a breach does happen.

What happens to my performance if your client base grows rapidly? Is your system scalable?
You should make sure your provider is monitoring the load on their servers and has a proactive plan in place to add servers if necessary.

How many clients do you have in your shared cloud computing environment?
Most providers offer a shared infrastructure. Make sure they have a significant number of clients using their cloud computing solutions. This demonstrates experience, client satisfaction, and scalability.

What is your largest client?
The answer to this question can help you determine whether the size of your firm is a good fit with the resources the provider has to offer.

How is your support team trained to protect the privacy of my data? What can I expect from them when supporting me?
The support team at any cloud computing provider should have strict procedures in place for protecting the privacy of your data, and they should be enforced consistently.

How can you help me optimize performance if my applications don't work well with your hosting?
Cloud computing providers should have technical experts on staff that know how to optimize application performance over the Internet.

How do you monitor your system performance?
Experienced cloud computing providers should have sophisticated tools for monitoring their servers and performance metrics. They should manage system availability and schedule system maintenance in a way that minimizes disruption.

What experience do you have with the accounting profession?
The accounting profession has a highly seasonal business. You want to make sure your cloud computing provider is sensitive to accounting busy seasons and deadlines. Make sure they offer extended support hours during busy season and that they limit system maintenance and updates during peak times of the year. Learning when they perform system maintenance should help you understand their experience with the accounting profession.

If I use your firm to store my cloud computing data, will it be accessible to anyone on the Internet?
There are two types of cloud computing services. The first type is public cloud computing, which hosts public applications like Yahoo and Google. These types of services are publically accessible via the Internet. The other type is called private cloud computing. These applications are restricted between the cloud computing provider and their clients who subscribe to the service. Most business applications are private cloud computing applications.

How will I be able to access my data?
You need to discuss the types of data access that your cloud computing provider offers. You should also discuss how you will receive your data should you choose to switch cloud computing providers and move your data to a new location.

Can I visit a data center to inspect the facilities?
Many data centers provide scheduled tours of their facilities. These tours will highlight the data center's physical security capabilities and technology. Firms are typically expected to pay the travel expenses to the data center for these scheduled tours.

Questions and Answers, continued

How do I protect my data if one of my laptops is lost or stolen?
The benefit of a cloud computing solution is that the software and data reside at the data center and not the physical laptops or devices used to access the applications. In some instances, data can be temporarily cached at the browser to improve overall performance of web applications. Through the use of password and browser management policies, access to cloud computing applications and cached data can be easily secured, even if laptops are lost. In addition, there are technologies that can remotely wipe data from a laptop after it has been identified as lost or compromised.

Should I be concerned about the security of public wireless Internet connections, such as those at coffee shops?
Each environment carries its own set of security risks, and public Internet connections are no exception. However, most cloud computing solutions use secure encrypted communications. These sophisticated encryption methods help ensure that even if someone does intercept your data, they will not be able to decipher it. To ensure that you are running an encrypted connection, simply look at the URL of the web address. It should say "HTTPS://," not "HTTP://."

Ready to get started?

Choosing a cloud computing provider is a big decision. But a good provider should be more than happy to answer your questions and help you find the right solution. And once you do implement cloud computing, you're likely to find that it's one of the best and most cost-effective investments you've ever made in your firm.

If you'd like to talk with a Thomson Reuters representative about our cloud computing options, or even get answers to general cloud computing questions, call us at **800.968.8900**, or email us at **CS. Sales@ThomsonReuters.com**.

TAX & ACCOUNTING

7322 Newman Boulevard
Dexter, MI 48130

T 800.968.8900
F 800.326.1040

CS.ThomsonReuters.com

THOMSON REUTERS