# CLOUD COMPUTING

# ALL THAT GLITTERS IS NOT GOLD


## SUMMARY:

Despite the term first being coined in 1996, it has taken almost 20 years for “cloud computing” to become mainstream.

And even though it has been widely adopted for personal use thanks to companies like Apple, Google, and Microsoft, the use of cloud computing in small and medium businesses (SMBs) is not as prevalent. This lagging adoption by SMBs begs the questions: “Why?” or “Why not?”

This white paper is one of a pair of whitepapers focused on answering those questions. First, it defines cloud computing. Then it outlines five risks a business owner should consider before adopting or using cloud computing.

In another whitepaper, we address the question of “why” and outline five reasons a business owner should consider cloud computing.



BIRMINGHAM CONSULTING
153-1235 Fairview St.
Burlington, ON L7S 2K9

## BACK TO BASICS

What exactly is “cloud computing”?

For anyone who saw the Terminator movies, “cloud computing” may conjure images of Skynet, an all-powerful artificial intelligence whose goal it is to wipe out the human species. If this is your perception of cloud computing, rest easy, cloud computing is not Skynet!

“Cloud” simply refers to the Internet, since the Internet is usually drawn as a cloud in network diagrams. So “Cloud computing” simply means “Internet computing”; or using the Internet to perform a function that would normally happen on your computer.

From a personal standpoint, using the cloud usually means storing your information on an Internet server that can be accessed from any device, anywhere.

Going one step further, with information stored in one central location, that server can make sure that the information on all of your devices is constantly synchronized.

*The concept of cloud computing is similar to mainframe computers used in the 1960’s, 70’s, and 80’s.*

This means that with cloud computing, your devices essentially become an extension of the Internet server to which they are connected. This is one of the reasons why devices like smartphones and tablets can seem to be as powerful as regular computers.

For anyone who is old enough to remember, the concept of cloud computing is similar to mainframe computers used in the 1960’s, 70’s, and 80’s – one large central computer with many terminals connected to it. The terminals could be local or remote; and often were in different cities.

Figure 1 - Cloud computing

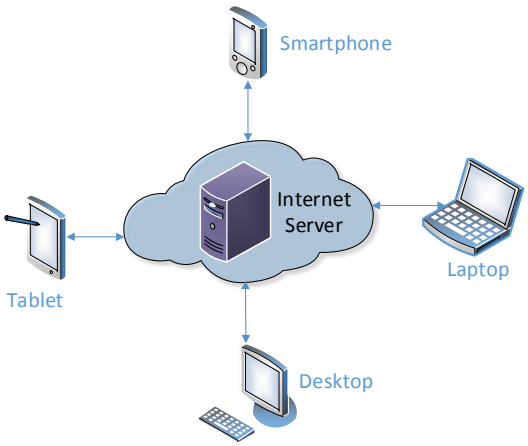
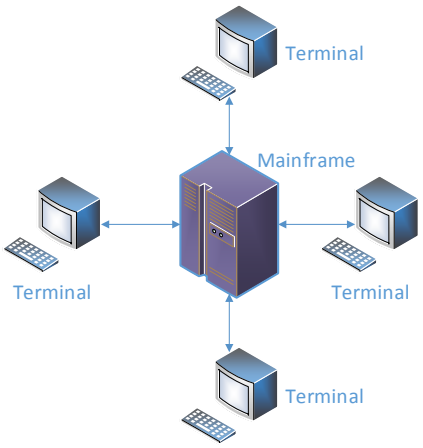



Figure 2 - Mainframe computer




Is cloud computing the same thing for business use that it is for personal use? Businesses have stored information on servers for years. Those servers were accessible remotely and some of them could even keep everything sync’d. So what’s different?

The key difference is that in cloud computing, the server is located somewhere on the Internet instead of at your facility. As a business owner, it means transferring some or all of the functions of your server to a server on the Internet. It also means taking advantage of servers on the Internet to perform functions that your server can’t.

## WHAT CLOUD COMPANIES TELL YOU

Cloud computing has "come into its own" in recent years; and according to industry experts such as Gartner Research, it will continue to grow in the foreseeable future for many good reasons:

- Little or no up-front cost.
- You can access your information from anywhere, on any device.
- Services are subscription-based.
- Services can be easily added or removed.
- Even more of your IT can be outsourced.

Chances are that you are already using some form of cloud computing, either personally or in your business. And chances are that you have experienced some or all of the benefits listed above.

But have you ever stopped to consider the potential risks of cloud computing to your business?

## WHAT CLOUD COMPANIES DON'T WANT YOU TO KNOW

If you do an Internet search for risks associated with cloud computing, the results tend to be focused on technical aspects of security; so they tend to be full of intimidating jargon that can be difficult to understand.

With that in mind, let's put aside the technical concerns and ask if there are any business risks associated with cloud computing?

Before answering the question, let's consider the following points that on the surface, may seem inconsequential; but when considered in the light of a business's legislative and privacy obligations, do they become significant?

With cloud computing…

- You, along with hundreds (or thousands) of other businesses, are storing your information on a server ***owned by someone else***.
- The owner of the server and the server itself is often be located ***anywhere in the world***, often offshore; and not subject to the same legal requirements as your business.

*All that glitters is not gold:*

*"Not everything that looks precious or true turns out to be so. Things…promise to be more than they really are."*

*- Wikipedia*

Now bear in mind that many employees also have personal accounts to store and share files (e.g. Dropbox, iCloud, SkyDrive, Google Drive, etc.). Since they are personal accounts, do you, as the employer, have any access to those accounts or any knowledge of what's stored in them and who they're shared with?

On a more basic level, could some of the direct benefits of cloud computing actually also be risks? For example, could the fact that you need the Internet to access your information actually be a liability?

How do all of these questions translate to risks for your business? Here are five to consider:

1. Complete dependence on your Internet service provider for your business to function.
2. Internal theft or "leakage" of confidential or proprietary information and intellectual property.
3. Ownership of and access to your information.
4. Inability to protect the privacy of your information, your employees, and your clients.
5. Long-term availability of your information.

As with any business, cloud companies promote the benefits of using their services and downplay any risks; but what would be the impact to your business if any of these risks became a reality?

## 1. Infrastructure Dependence

### Reliability

One of the compelling reasons for a business to move to the cloud is that applications and information are available anywhere you have an Internet connection. But this also means that from within your office, the only way to access anything is via the Internet.

In Canada, specifically within the Greater Toronto Area (GTA), most businesses rely on 100-year old phone infrastructure for Internet access. Experience has shown that with this infrastructure, there is a good chance that your business will randomly lose Internet access for up to one hour per month.

*Most businesses in the GTA rely on 100-year old phone infrastructure for Internet access.*

Without cloud computing, when your office loses the Internet connection, you are unable to check email and you can't browse websites; but you can still work within applications on your computers and any in-house servers. With everything moved to the cloud, you can't even open an application like Word.

What would be the impact to your business if no computer work could be done for an hour every month? If the outage could be predicted or scheduled, the impact would be low; but when it's random, Murphy's Law tends to dictate the timing and the impact.

### Speed

Old infrastructure also dictates the speed of business Internet. Unlike residential Internet, availability of fast Internet for business is not as widespread.

*Murphy's Law:*

*Anything that can possibly go wrong usually does.*

*- Wikipedia*

This translates to the probability of your business Internet connection being less than half the speed as home Internet.

This speed difference is generally not a problem for browsing websites and downloading files; but if you are using cloud services that require information to be transferred from your office to the cloud, it can be a significant bottleneck. The Internet will be at a crawl when those "uploads" are taking place.

## 2. Information Theft or Leakage

Have any of your employees ever created an account with a service like Dropbox, SkyDrive, iCloud, or Google Drive to access work-related files from outside the office?

If the answer is "yes", bear in mind that even though the files may be owned by the company, the account in which they are stored is owned by the employee.

When the account belongs to the employee, not to the company, as the business owner, ask yourself…

- Do I have any access or control over that account?
- What other devices are sync'ing with it?
- Who has direct access to that account?
- Are any folders or files being shared with anyone who shouldn't see them?
- What is my liability if that employee fails to adequately protect the account?
- If the employee closes the account, do I have a copy of the files on any company computer?

None of these questions matter if the information is mundane or publicly available such a product data sheets, published whitepapers, marketing brochures, etc.

However, what if the employee has stored sensitive information in the account? For example: client information, internal documents, intellectual property (IP) information, anything you wouldn't want a competitor to know?

Such confidential information could be inadvertently or intentionally made accessible to other parties (i.e. "leaked") by the employee *at any time* without your knowledge or consent. The most vulnerable time for such a leak is when an employee leaves the company, regardless of whether the parting is voluntary or involuntary.

If the employee has chosen to leave voluntarily, he or she may want to take a copy of your client list so that they can call on your clients. Maybe they are leaving to go to a competitor and they want to take a copy of your new product design.

*The most vulnerable time for an information leak is when an employee leaves the company.*

No matter what the information is, all they need to do is make sure there is a copy of the relevant files in their personal cloud account and they will have access to the information after they leave your employ.

Not only could this hurt you competitively, it might also create legal liability for you if the information contained client personal information such as home phone number, home address, date of birth, etc.

Why would you be liable? Because that information became accessible to an outside party, *via your company*, without the client's permission.

The situation could be even worse if the employee left involuntarily. They might company have important files in their cloud that don't exist anywhere else and in their anger at being dismissed, delete them.

How do you as a business owner protect yourself against these scenarios?

Answer: In layers, using employment contracts, policies, procedures, and technology. Consult with HR, legal, and technology experts to determine your best defense and to develop response plans, should something happen.

## 3. Safeguarding Your Information

Have you ever used a self-storage unit? If you have, you know that you're renting space in someone else's facility; and you're going to store things there. You don't own the facility – you just want to store your stuff there.

Both the landlord and you are responsible for security. The landlord provides the fence and controlled entrance; and trusts you not to disclose the passcode. You're entrusted with the passcode and place your own padlock on your unit.

When cloud computing is used to store information, it's similar a self-storage unit: You're renting space on some else's server to store your information there.

Both you and the service provider are responsible for security. The service provider is responsible for protecting the server and you have your own username and password to protect your information.

*The origin of cloud storage.*

But here's where things change.

With a self-storage unit, you retain ownership of your things (unless you default on payment) and only you have the ability to access your stuff.

How would you feel if a self-storage operator was allowed to go into your unit at any time and use your stuff? They could take pictures or videos of it and share it with anyone they chose. And you were powerless to stop them because they granted themselves the right to do so in the fine print of the rental agreement?

Sounds incredulous, doesn't it? But if you look at the fine print of many cloud service agreements, you'll find such terms. Some will outright tell you that *they now own your information*; while others sugar-coat it by saying that you own your information but you grant them the right to look at it and use it any way they please.

Without naming names in order to protect the innocent, there have been recorded incidents of personal dental records showing up in Internet search results. The records were stored with a large cloud service provider whose terms of use allowed them to use everyone's information any way they wanted.

The bottom line is that as a business owner, you need to be aware that by moving to the cloud, you may be jeopardizing employee, client, or patient confidentiality, unknowingly sharing your intellectual property, and unknowingly sharing internal documents..

Be sure to read the fine print before using any cloud service.

### Password Resets

Another consideration when it comes to safeguarding your information: If you forget your password, how do you get to your information?

If the password can be reset by the cloud services provider (i.e. their support), chances are it could also be reset without your knowledge – meaning that it could be changed by someone else in order to access to your information.

The likelihood of this occurring is pretty slim; but it's another consideration when deciding what should be in the cloud.

## 4. Privacy Protection

Where does your information go when it's "in the cloud"? As explained earlier, it's on a server somewhere on the Internet. But where is the server? Is it in Canada, the U.S., U.K., India, Russia, Ukraine, Romania?

If it's not in the same country as your business, your information is subject to the laws of that country; which may be different than the laws you're subject to; and you might find yourself in violation of local legislation. Therefore, it's always a good idea to learn the location of the backup server before entering into an agreement.

Figure 3 - Legal jurisdictions


## 5. Availability

We all understand that having your business depend on a single large client is risky. What happens if that client chooses to take their business elsewhere?

It's just as risky to have all of your business operations depend completely on the viability of a single company. If you've moved all of your systems to the cloud, what happens if that cloud company fails, gets purchased by another company, or is affected by Internet volatility?

The implications of a company failing is pretty obvious; and one would hope that during an acquisition, the purchaser would continue to offer the same services. But what is Internet volatility?

Internet volatility can range from something as simple as the chain between you and your information being temporarily broken, to being an innocent victim of 3rd-party activities.

An example of 3rd-party activities can be found with the recent case in which Microsoft seized assets of another cloud company based on the perception that customers using the services of the cloud company were conducting illegal activity. Understand the distinction here: the cloud company did nothing wrong, some of its users did.

*"Critics blast Microsoft's takedown of No-IP domains""*

*- Computerworld, July 2014*

However, when Microsoft seized the assets, thousands of other users were suddenly unable to access their accounts and their information for days while lawyers argued in court.

What if something like this happened to you after you moved all of your business into the cloud? Could you conduct business for days without access to your information, whether it be financial information, email, sales software, marketing programs, or whatever? If not, what would the impact be to your business?

## CONCLUSION

Cloud computing is not a new concept; but it is finally becoming available and useful to SMBs. However, with this technology come some inherent risks:

1. During Internet outages at your office, the entire business could be shutdown, not just email and access to websites.
2. Cloud computing makes theft of information by employees very easy.
3. You may be giving up complete ownership or usage rights to your information.
4. The privacy of your business and client information may not be protected.
5. Your entire business is now completely dependent upon the viability of another company.

So why would a company move to cloud computing? There are a number of reasons. Before you make a decision to move to the cloud, we recommend that you weigh the risks along with the benefits and consult with a professional.

The benefits associated with cloud computing are discussed in this whitepaper's twin called "Cloud Computing: Reduce Costs and Improve Productivity", available from www.birmingham.ca.

To determine if cloud computing is right for your business, contact our consulting group or a no-cost evaluation:

Birmingham Consulting Inc.
289-895-8948
info@birmingham.ca