

What is “Cloud Computing?”

- Terminology:
- “Cloud Computing” is a made-up term that is sometimes used by technical computer people.
- However, it is not a technical term.
- It is a term that was made-up to try to allow non-technical people to understand a concept that is very technical.
- If you think about it, the last place that you would be able to see and navigate clearly, would be a Cloud.
- It is a term that has been used in recent years by business executives as a money-making tool because it is so ambiguous.
- Part of the current popularity of Cloud Computing is based on ignorance of how Cloud Computing actually works. Business and Sales executives are banking on people having difficulty understanding the technical details. Their goal is to make money----Their goal is NOT to make your business safe.

How Does it Work?

- A company (provider) buys a large number of high-performance storage computers.
- This company then buys a direct connection to a main Internet pipeline.
- Your company buys so-called “expandable” storage room from the provider who then provides your company with Internet access to their storage location.
- The provider will have a main location in a city; but then they will build (or lease) multiple locations in extremely low-cost areas, such as Wyoming, and will be able to store your data at that location for a fraction of the main location cost. Your data will be sent over the Internet by both your company and the provider.
- Because your data does not reside in one location (in many cases) it can be sent anywhere, hence the ambiguous term, “Cloud Computing;” the provider will be storing their customer’s data in a Cloud meaning that you cannot see or know exactly where that data might reside.
- Once your company sends its data to the provider all control over the security of the data is passed over to the provider.
- During the data transmission process, which is across the Internet, your company loses all control of that data.
- However, data transmitted across the Internet using SSL (Secure Sockets Layer) is nearly impossible to de-crypt.

Current Cloud Computing Models

- Current Cloud Computing models present the business owner with a proposition based on “saving money.” The idea is that a company should cut back on IT staffing and IT machines and instead let someone else pay for that expense. A business is presented with the idea that someone else can provide unlimited storage amounts of data room and that they can also provide the computer applications that a company uses, such as the Microsoft Office Suite or even proprietary applications.
- While this is true, there are fundamental problems associated with the model. As stated above, once you allow a Cloud Computing company to “host” your data, they own it. You will be sending and receiving your company’s private data across the wide-open public network, the Internet.
- The Cloud model as implemented by the provider, can and will spread your data across a wide number of locations. In fact, some or all of your data can end up being split across multiple machines.
- If you went to the provider and asked them for the exact physical location of your data, they would have a difficult time showing you the exact machine where your data was located. This is why it is called Cloud Computing---because your data disappears into a cloud!
- If you use applications that are hosted by a Cloud provider, you must be aware that it is possible for that provider to see and log everything that occurs when the application is being used.
- It would be nearly impossible for you to guarantee that your data was wiped-clean off of the provider’s machines if and when you decided to leave or change your provider.
- There is no way for your company to assure that someone at the provider is not replicating your data for their own gain.
- Concentrating a large number of different companies mission critical data under one provider provides for an enriched target for data criminals and their networks.

Basic Rules of Data Safety

1. Own the machines where your company data resides. Own the location and security where the machines reside.
2. Assure that your company data resides on an internal network that is not directly accessible by anyone.
3. Do not assume that anyone outside of your company can assure your company's data security. If they do not work for your company, they do not have a primary reason to protect your data.
4. Separate your company's data storage from any and all computers in your company that are connected to the Internet.
5. If your company is not open and operating on evenings and weekends, disconnect your business from the Internet at the incoming line when you close and go home.
6. Identify all company-critical data and assure that it is replicated to a storage device that you own and know how to operate successfully.
7. Understand that the Internet has no rules, no laws governing it's use and no one overseeing how it is being used in relation to your use. The Internet is a wide-open information pipeline that is inhabited by as many dishonest people, as by honest people.
8. In today's world, Internet criminals are highly organized, have huge budgets and are ruthless.
9. Nothing is truly free. Providers will offer 2 GB of "FREE" storage space. 2 GB of storage space can easily hold any company's entire financial data. Therefore, storing your company's financial data with a provider is about the same as turning over your IRS tax records and all of your Credit Card information in a manila folder to a perfect stranger on the street to keep safe for you.
10. Having your own secure server on which to store all of your company's financial data is just like having your own safety deposit box. Only you have the key and you are the keep-safe of your data.