AVAWARE
TECHNOLOGIES

AVAWIRE

AVAwire Articles: The Cloud Collection

A Collection of Articles from the AVAwire Newsletter Pertaining to Cloud Computing

Cloud Computing: the Sky's the Limit for File Sharing Possibilities

It seems like only yesterday that computers themselves were considered an innovative and novel concept in the workplace. Desktop PCs, laptop computers, corporate networks, the internet…. If all that's not enough, now the technology industry is truly reaching for the clouds.

If there's one thing everyone can depend on with the technology industry, it's change. No sooner does one get used to the latest and greatest innovation, but another emerges making us all wonder how we ever lived without it. No sooner than most companies have gotten comfortable with the idea of trusting centralized fileservers with their most sensitive data, have they begun to flirt with obsolescence. At first this may seem somewhat extreme, but make no mistake about it – the movers and shakers of the technology industry don't think so.

For those that haven't been keeping up, "cloud computing" is basically a very simple concept; Instead of companies or individuals owning and maintaining their own internal fileservers, why not set up a really big one that can service a whole lot of people. The notion may seem unrealistic, but it's actually neither impractical nor entirely unprecedented. One would be hard pressed to find any company or organization that doesn't have a web site today. In fact, even individuals often find it useful to set up their own personal web "presence" to share files and photos with friends and family. Of all those web site owners, how many actually own and operate their own web server? The overwhelming majority find it far more practical and economic to simply "rent" space on someone else's server (i.e. a web hosting company). Companies such as *Microsoft*, *Amazon* and *Google* are attempting to extend the same principle to the rest of the enterprise. Meanwhile, the more consumer-oriented companies such as *Apple* and *Microsoft* (again) are doing the same for the individual.

Here are just a few examples of how the major players are bringing cloud computing to the masses:

Company	Consumer Offering	Enterprise Offering
Apple	iCloud is the newest, well-publicized service from *Apple* that offers each of their users 5gb of complimentary space in their “cloud”. This space is used automatically by *Apple*’s applications to store and share backup copies of documents and photos. *Apple* even allows people to store their entire music libraries online – for access anywhere there is an internet connection.	None
Amazon	Like *Apple*, *Amazon* also offers their users free storage space on their servers to store their personal files as well as any music they wish to upload or purchase online. *Amazon* automatically places a copy of any music bought through their music store on their user’s “Cloud Drive” and allows them to play it back with a special “Cloud Player” application.	*Amazon Web Services (AWS)* is a leading provider of cloud storage to corporations and developers.
Google	*Google* also offers complimentary cloud storage to their users and even provides free office-type applications that can be used online and store user data in the cloud.	*Google Storage* is *Google*’s offering to the enterprise and developer community.
Microsoft	*Microsoft* lead the cloud storage trend with the introduction of “*SkyDrive*”. Their product offers the best of many of the others. Naturally, *SkyDrive* can be used to hold personal data and music; but it can also be used to automatically synchronize operating system settings and configurations between multiple PCs. The upcoming *Windows 8* will utilize *SkyDrive* to facilitate a number of impressive new features.	*Microsoft*’s ‘*Office 365*’ product allows small companies to have access to *Microsoft Exchange*, *Lync* and *SharePoint* servers without the considerable expense and effort of setting and maintaining up their own. (Typically this type of endeavor requires full-time I.T. staff.)

Note: *This table is not intended to be comprehensive. It merely provides a sampling of some of the services offered by a small group of well-known companies.*

Even beyond these companies, there are many other service providers that want to rent out a piece of their cloud. *DropBox* is just one example of a company that has had incredible success in the cloud storage space. Unlike many of the "major" companies listed above, *DropBox* only offers 2gb of free storage. Why have they become so popular then? Their success is undoubtedly due to the exceptional "client" software they offer on virtually every major platform out there – from desktop to mobile. Just to be clear, a "client" in this context is a piece of software that allows users to actually access and make use of the cloud storage. Nearly all cloud storage providers offer a web interface that allows users upload or download files though the use of a web browser. Some, like *Apple* and *Amazon*, offer highly specialized apps such as their cloud-based music players to access the data stored online. *DropBox* has done an exceptional job of creating elegant client applications for *Windows*, *Mac OS X*, *Linux*, *iOS* and *Android* that allows users to manage their cloud storage just as though it were any other folder on their hard drive or network. *DropBox* even allows users to selectively share individual folders with others; a feature not currently being offered by any of the major vendors.

There is no doubt that cloud-based services will have a tremendous impact on the way many companies do business in the years to come. For the time being, it is certainly well worth exploring how some of these often-free services can open up incredible new possibilities for the way we manage and share information. At the very least, it brings a number of server-based technologies into the reach of many companies that previously couldn't justify or afford them. Until recently, companies that wanted the benefits that came with corporate LANs (local area networks) or WANs (wide area networks) were faced with daunting financial prospects, beginning with employing in-house I.T. staff to maintain everything.

To be fair, cloud-based services are not ready to completely eliminate the need for local fileservers. One must bear in mind that the usefulness of a cloud-based system is entirely dependent in the quality and speed on ones internet connection. At the best of times, transfer speeds will be considerably slower than what most are used to. With time, however, and with improved connectivity we may all see the day where local fileservers and network hardware may become a thing of the past.

Once thing is for certain: if anyone thinks cloud computing won't touch their business in the near future, then they've truly got their head in the clouds.

AVAwire, March 2012

The “Cloud” takes Project Sharing to New Heights

While most competing products are limited to embracing decades-old client-server platforms for storing data, AVAproject offers a discrete file format that makes projects is just at home the “clouds” as they are on the network. Designed with complete portability in mind, AVAproject files are ideal for this powerful new computing paradigm.

Networks are wonderful things. In fact, one could argue that they are an absolutely essential part of any modern business operation. The important thing to remember is that there is a difference between network-capable and network-dependent. **AVAproject** and **AVAcad** are designed for both flexibility and portability. Although server-based environments have many obvious advantages, too often the way in which software is implemented on them is far too restrictive.

You would have to have been living in a cave for the past few years to have not noticed that mobile computing is a reality that is here to stay. Most PC users have realized that it’s not enough to be able to move around within a building, but they want complete portability for themselves and their data.

Server-based applications typically answer the call of mobile users by suggesting a connection via the internet. A VPN (virtual private network) is simply an encrypted data connection made across the public internet. This is all well provided the server is up, the VPN appliance is working, the internet connection is solid and the location where users find themselves support VPN connections (not all cellular or public access points do.) Clearly this is a complex solution to a simple problem. Even if one were to accept the costs of setting up and maintaining such a configuration, they would be at the mercy of system failures, poor internet connections or inflated roaming charges.

The obvious solution is the one employed by most major software developers. Following a model used by companies such as *Microsoft* (for their “Office” applications), **AVAware** uses discrete files to hold project data. What this means is that like *Excel* or *Word* files, **AVAproject** files can be copied to flash drives, emailed to colleagues or… stored in the cloud. For those users that wish to share data in a network environment, that is certainly possible. As previously mentioned, those **AVAproject** files are right at home just about anywhere! Many people store projects on company fileservers so that they can be accessed by multiple users while some even use management systems such as *Microsoft SharePoint* to administer the sharing.

A truly exciting new technology has emerged in recent years that offers another powerful option for companies interested in sharing projects beyond the confines of a building. The best thing about this option is that unlike the multiple servers/VPN solution, it’s often completely free of cost!! Sound interesting?

As discussed in our previous tech-article about cloud storage providers, there is one in particular that is particularly ideal for use in project sharing. *DropBox* is free/low cost cloud storage platform with a *Windows*-based “client” application that makes using it nearly effortless. Upon signing up for an account, each user is given 2gb of storage space for free; additional space can be “rented” as required. Quite honestly. 2gb holds a lot of projects! The really great added feature of *DropBox*, however, is that individual folders can be shared between users. Within a user’s “*DropBox*” folder, any sub-folder can be designated as “shared”, allowing other selected users to access the files it contains. In effect, this is a “network share – in the sky!”

The “discrete” nature of **AVAproject** files is the final component that makes this global file sharing solution possible. Files can be saved to a *DropBox* folder just like any other network drive. Once the *DropBox* application has completed synchronizing it with the cloud, it is available for colleagues to access or to retrieve from other locations (i.e. home).

There are several other cloud storage solutions available today, and more emerging constantly. This technology is the next logical progression of the “wired” internet. Mobile computing and the call for the general portability of data is causing many software designers to re-think their outmoded practice of anchoring users to a single file server. Like other emerging computing technologies, corporate networks should be thought of as a tool for enterprise users – not a leash!

AVAwire, March 2012

Cloud Computing: Keep Your Data in the Clouds – and Your Head Out of Them!

In last month's AVAwire, we discussed the growing trend in cloud computing and all the benefits that come with it. As groundbreaking as this technology is, it's not without its pitfalls. We would be remiss if we didn't also point out some items of concern.

There is no doubt that cloud computing is one of the most revolutionary concepts to hit the software industry since the invention of the hard drive. Many companies have embraced "cloud" or "off-site data storage" providers as being their alternative to a life of screwing servers into racks. The upfront benefits to off-site data storage a certainly enticing; instead of investing in all that expensive server hardware and the people to maintain it, let the cloud provider take care of all of that. For multi-location companies, the benefits are even greater; instead of configuring complex wide-area networks and VPNs between locations, one can simply access a shared cloud from anywhere.

This is all true. No doubt about it. The cloud is definitely the way to go… all aboard! Wait.

As beautiful as any cloud looks, they usually come with a little rain.

Before we all throw our servers into the bin and begin uploading our companies' wealth of intellectual assets into the cloudy heavens, perhaps we should take a closer look. Although we use the term "cloud", that's obviously not where our data is going. Instead of being safely housed in a server in our back rooms, our precious data is now "safely" being stored in servers in someone else's back room. This is an important thing to keep in mind. We often hear people say that one should consider anything they post on the internet as being defacto "public". Why then is everyone so ready to believe that cloud storage is safe, secure and beyond the reach of prying eyes?

By no means should this be considered a claim to having knowledge of illicit activity, but the fact remains that data storage providers warehouse data in 'data centers'.

People work in data centers. Curious and often financially motivated people work in data centers, and they have access to data they are responsible for maintaining. Period. Anyone who's worked in a government office or a financial institution knows how much personal data is available at each employee's fingertips. We've all read stories in the news about employees at video stores 'leaking' public figures' rental histories to the press, etc. The fact of the matter is that the moment your data leaves your machines, it's out of your control.

Many will argue that much of this risk can be mitigated by using private encryption keys. True, but without launching into an entirely different debate let's all simply acknowledge that no measure of security has ever been proven perfect. That having been said, before committing all your company's valuable data to the care of a third party, it's important to consider what the ultimate impact of that data being made public would be to your company.

In addition to security, the other issue is that of reliability and accessibility. Just like any other utility provider, when your cloud service goes down you're out of luck. If you're used your trusty I.T. staff to keep your network functional and your employees working in the event of failures, those days are over. Just like any other utility provider, when your cloud service goes down the only answer you're likely to get is "we're working on it". Seriously, data centers serve a lot of customers. You individual concerns are not going to mean a lot to a company the size of *Microsoft* or *Amazon* – no matter how important it is to have that bid in on time. The entire computer industry was taken by surprise when Microsoft's new cloud-based service "*Office 365*" went down on February 29th dues to a leap year bug of all things. Their entire user base was unable to access their email or office documents until they got the matter sorted out. Generally speaking, these providers do a good job, but the fact of the matter is that your data, and as such, the operation of your business, is out of your hands.

For these reasons, there are a couple considerations one should keep in mind when contemplating any off-site solution. First and foremost, consider the stability and reputation of the company you're entrusting with your data. Ask yourself if you would trust that company to safe-guard your most valuable assets.

Second, and most importantly, don't rely on any storage solution (cloud-based otherwise) as your *only* one. As wonderful and accessible as the cloud is, keep far away from any solution that does not allow you to maintain an up-to-date and current local copy of every piece of data your company owns. It's your data after all, take good care of it.

Don't take this small dose of reality to mean a condemnation of all things cloud-like; in fact, cloud-based computing is truly every bit a revolutionary as it appears. We just want our valued customers to approach any new technological implementation with their eyes wide open and (we had to say it) their heads out of the clouds.

AVAwire, April 2012

Software as a Service: Who's Got the Keys to Your Data!?

In last month's AVAwire, we discussed the growing trend in cloud computing with all its benefits... and its potential pitfalls. On the heels of the cloud-based computing phenomena, another not-so-new idea is gaining renewed interest.

"Software as a Service" (SaaS) is not a new idea. Software developers have been exploring this idea since the internet began gaining acceptance in the corporate workplace in the mid 1990s. The actual concept is simple enough; instead of buying software in the traditional sense, the developer essentially "rents" the software to their customers. Normally, the developer/vendor sends out a disk (or download location), and the customer installs the software on their own PC or PC network. In a SaaS situation, there is no software to install, users simply log into a website and use the software online.

This arrangement offers a number of the same benefits as cloud storage, in addition to a few others. There's no need to install and maintain software locally, software updates are automatically performed by the site operator, software can be accessed from anywhere there is an internet connection, etc.

As it seems with all new technologies, upon closer examination there are several issues of concern that could make SaaS a poor choice for a corporate environment.

- The first problem: the client doesn't actually *own* anything! This may be fine for minor utility applications or games, but bear in mind that your business may become dependent on something that is never under your control.

- Although it may sound convenient to have updates performed automatically, this also means that you have no choice as to when this occurs. If the vendor decides to put a new software version online, the customer and their users must adopt and possibly stop to learn the new version immediately. There is no way to put this off if the timing is inconvenient – you are now on the vendor's schedule.

- The ability to access the software "anywhere" also comes with the other side of that coin: the software can only be accessed if and where there is a solid internet connection. Naturally, the quality of the connection will determine how effective and productive the work experience is. If the internet goes down, or is running slow at the moment, work may come to a stop.

- Most PC users have had to deal with computer or network breakdowns at one time or another. Nothing is more frustrating than having to deal with a workstation becoming unavailable right when there is a job coming due. In a SaaS situation, that possibility is further aggravated by the fact that getting the software back online after a failure is in the hands of an outside party, in a far away location that is usually out of reach. If your PC goes down, you can always grab your install disk and move to another machine, when using a web-based application you have no choice but to wait for it to come back online.

- The largest issue, and one that many forget to consider, is that *your data* is sitting on that distant web server along with the application that accesses it. If your business deals with sensitive or confidential data, then you should ask yourself who actually has access to your private data. Many industries (medical, etc.) are even prohibited by law from using web-based storage or services that are not independently certified. Federal and state regulations have been enacted to protect sensitive information. Two such examples are the Health Information Technology for

Economic and Clinical Health Act (HITECH Act) and new updates to the Health insurance Portability and Accountability Act (HIPAA).

To sum it up, the majority of the concerns stem from the fact that SaaS arrangements place the customer entirely at the mercy of the software vendor. If that vendor is a nationally recognized company, then there is probably less of a reason for concern. On the other hand, when dealing with small, independent vendors one has to wonder "Who's holding the keys?", and, do you trust them to safeguard your valuable data?

The final consideration is one of access. Should that web server become inaccessible, due to equipment failure or the company discontinuing operations, you may find yourself unable to access any of your data or the application your company has come to depend on. There is no doubt that cloud/web-based storage and software offer exciting new capabilities, but at the same time one should be aware of the potential issues that may bring with them.

AVAwire, May 2012

Cloud Services Hacked & Social Engineering Reveals Massive Security Failures

In a recent issue of AVAwire, we discussed several causes for concern and areas or potential risk for those who relied on cloud-based services to store their vital data. Not to say "we told you so", but several service providers have recently experienced instances of "hacks"' and other of "security failures"!

The past month has not been kind to the cloud. Several popular online services have reported incidents of "hacking", some resulting in substantial data loss for unfortunate users.

200,000 LinkedIn Passwords Reported Cracked [1]

In early June, Vicente Silveira, Director at *LinkedIn* confirmed that 200,000 passwords had been hacked and reportedly sent emails to the owners of all the compromised accounts giving details and instructions on how to reset their passwords. Users were advised to not only change their passwords on *LinkedIn*, but on any other service where they used the same ones.

Reuters' Twitter account hacked [2]

The Reuters news organization reported that their *Twitter* account (@reuterstech) was commandeered by hackers and used to disseminate pro-Syrian government tweets. No details were offered as to how this was done, but the account has been suspended pending a complete investigation.

Several Hundred Dropbox Accounts Hacked [3]

On July 31st, the popular cloud-based storage service *Dropbox* reported that hackers had accessed data in several hundred unsuspecting *Dropbox* users' accounts. It was suggested that third party sites were responsible for allowing malicious individuals to gain access to usernames and passwords that allowed them to sign in to the various *DropBox* accounts.

A Call to Apple Support Results in a New Father Losing Photos of His 18-Month Old Daughter! [4]

Although only one person was affected, perhaps the most devastating hack in recent times was a lesson in dangers of "Social Engineering". *Gizmodo* techology journalist, Mat Honan was playing with his baby daughter when suddenly his *iPhone*, *iPad* and *Macbook* computer all suddenly went dark! It seems a hacker obtained information through phone calls to *Amazon* and *Apple* technical support that allowed them to gain access to several of Honan's online accounts – including his *Apple* ID. All this was done in an effort to hijack Honan's enviable 3-character *Twitter* handle (@mat).

In order to prevent him from resetting his own password and ensure that there was sufficient time for the hacker to complete the task, the hacker used *Apple*'s 'remote wipe' feature to completely empty the contents of all his connected devices and his *iCloud* backups.

The really unfortunate result of all this was the loss of all the pictures that the new father had taken of his 18-month old daughter thus far. Reportedly, all his accounts have been restored but the pictures have not.

The reason we're bringing these incidents to the attention of our clients is simply this – to demonstrate that IT DOES HAPPEN! All of these hacks occurred in just one month and there's no telling how many other incidents may have occurred in the same time period. It's only because of the rising trend in online computing that stories like these are getting reported at all.

We realize that articles (such as the one we published recently outlining the potential pitfalls associated with cloud computing) can appear somewhat pessimistic, but the reality is: These things do happen. Not only do they happen, but they are doing so at an increasing rate.

Users must recognize that cloud-based computing is a brand new technology and should consider the possible ramifications carefully and take the proper precautions before entrusting sensitive or confidential data to such a service.

[1] Source: "LinkedIn Confirms Account Passwords Hacked", Ian Paul, PC World, Jun 6, 2012
[2] Source: "Reuters Twitter account hijacked, fake tweets sent", Steven Musil, cnet.com, Aug 5, 2012
[3] Source: "Dropbox confirms it was hacked, offers users help", Dana Kerr, cnet.com, Jul 31, 2012
[4] Source: "Allowed Hackers Access To User's iCloud Account", forbes.com, Aug 5, 2012

AVAwire, July 2012

AVAware Tip: Securing Your Data in the Clouds

Normally this section of AVAwire is dedicated to showcasing tips and techniques aimed at assisting users of AVAware software work even more efficiently. Given the recent security issues experienced by various online and cloud-based services, we thought it appropriate to offer a bit of a departure from our usual fare.

A Brief History of Hacking...

We've all seen that character in every crime drama – the one that can "hack" into anything from police computers to elevation control systems in a matter of seconds. Good news: such a person does not actually exist. Hacking is more about systematic attacks and "social engineering" than about knowing some super secret sequence of keystrokes that will make a user account pop open faster than you can say "Open Sesame!"

Systematic Attacks (a.k.a. The "Brute Force" Method)

The classic brute force approach to discovering a password involves nothing more sophisticated than a library of common words, names and phrases that hackers will attempt against a given user name in every possible combination. Resourceful hackers will even "customize" attacks on individuals by adding words, names and dates that they know relate specifically to the person they are targeting.

Social Engineering

The most common (and completely non-technical) approach to discovering user names and passwords is referred to "Social Engineering". This is simply a fancy way of saying "tricking someone into letting you in". Classic forms of this "hack" involve people calling unsuspecting users and claiming to be a support person, a co-worker from another location, a bank employee, etc. It is surprising to find out how many people are willing to provide confidential information if just asked the right way.

A type of "game" is played every year at the annual DefCon hackers' convention in Las Vegas. A "hacker" is placed in a sound proof booth and given a specific amount of time to call various business and attempt to trick the people at the other end of the phone into providing access to user accounts. They are always successful, and always in a matter of minutes!

Given this information, the real question is "What can a person do to protect themselves?" The following is a short list of simple ideas that can help protect your online presence from becoming the victim of a hacker. Please bear in mind, although some of these ideas may seem obvious – if more people actually took these precautions there would be fewer security breaches.

Use Secure Passwords

Your password is your first line of defence against the simplest form of hacking. Experts suggest using passwords with at least 10-12 characters, being sure to combine numeric as well as alphabetic characters. Also, don't be afraid to incorporate symbols (+-/#$%&) into your password whenever they're allowed by the system you're securing.

Be certain to avoid names and dates that are specific and personal to you. If you know them, then it's likely that other people will as well. Celebrities have had their accounts hacked because they've used names for passwords that could be found on fan sites and Wikipedia!

Also, remember those resourceful hackers that will add your personal information to their systematic attack libraries. If you think that simply combining your spouse's name and your mother's birthday results in an unbreakable password – think again!

Lie on the "Security" Questions

Many systems (i.e. banks) use secret security questions to verify your identity. Most will let you select the question, though most offer a list of acceptable choices. The problem is that the questions usually have answers that anybody who knows you will also know the answers to. Questions like "Where did you go to school?" and "What is your mother's maiden name?" are NOT secure. You are far better off deciding on a fictitious answer that no one else would ever guess and use that. Remember, no one insists on the answer to these questions being true – they only have to match the answers you gave when you set up your account.

Use Multiple Passwords and Email Accounts

The biggest mistake most people make is to use the same password on multiple sites and accounts. This is never a good idea. Obviously, should a hacker get lucky and gain access to one of your accounts, they suddenly have access to all of them.

Most systems require you to provide an email address that they can use to send password reset links when necessary. Do not use the same email address for all your accounts for the same reason you wouldn't use the same password. If a hacker gets hold of your email account, they can request password resets for every system for which you've used that email address to setup an account.

Use "Two-Factor" Identification Where Available

Simply put, "two factor" identification requires two pieces of information to log into a given account. Usually this is a password and a numeric code that is either sent to your phone via SMS or a rotating number that you are given ahead of time.

This type of login is certainly more inconvenient, but infinitely more secure and virtually unbreakable!

Educate Your Friends and Employees

The only line of defence against social engineering is education. Meet with your staff and discuss this growing trend; make sure they know not give out confidential passwords to ANYONE they don't know, no matter how good the story sounds. Remember, these types of hackers are experts and have surprisingly good results even when dealing with intelligent people!

Beyond that, make sure everyone you know knows that companies like Microsoft and especially your bank will NEVER phone up and ask for a password... EVER!

When All Else Fails... BACKUP, BACKUP, BACKUP!

Despite everyone's best efforts, sometimes the unfortunate happens. When it does, the only thing you have to fall back on is often secure backup copies of your data.

Effective backup practises is a topic for its own article, but briefly there are a few things to keep in mind. The ONLY form of backup that can never be hacked is one that NOT connected to anything. For that reason, never rely on any cloud-based storage solution as your only backup. Removable hard drives cost less than a hundred dollars and will instantly become priceless should you ever find yourself staring at an empty hard drive or cloud account.

With all that said, always bear in mind a little paranoia can be a good thing. Although security often comes at the cost of convenience, please consider the implications to your business and your life in general should you become the victim of a hack.

AVAwire, July 2012

AVAware Technologies
2897 Brighton Road
Oakville, Ontario
L6H 6C9

Phone: (416) 239-9099
Fax: (416) 239-9199

http://www.AVAware.com