Issue 36

February 2012

Page 1 of 2

THE M&H MONITOR

M&H CONSULTING

Never Buy a PC or Server Again

Tom Harriss

Keeping your computer network up to date is one of the hardest and sometimes riskiest parts of your business. Over the past three years we have gotten many inquiries about cloud services from clients looking to break the cycle of continually buying and maintaining more and more equipment, which sits there and grows obsolete whether you use it or not. However we have always advised a strong dose of caution against jumping too quickly into the cloud, as the risks and expenses tended to outweigh the rewards... at least until now.

One of the first concerns has always been the available Internet connection. Until recently Internet speeds have not been fast or reliable enough to handle cloud services, and in some locations that is still the case. But where services like Verizon FIOS have become available, this concern is no longer an issue.

Another concern has been the security of your data and the reliability of the hosting company. While this concern will never fully disappear with any Cloud service, we have seen the market mature to a point where these risks have faded and are no longer a barrier for the mainstream use of Cloud services.

In the end, the largest and most important hurdle has always been cost. In order to use most of the current cloud services you still need to have a server, and computer at each desk, maintain it, and in many instances, keep separate cloud providers for email, data backup, remote document storage and access, etc. While some problems were solved by the cloud, the added costs just didn't make sense for those without special niche needs.

But being very aware of the ever growing interest in the many benefits brought by moving to the cloud, we have constantly monitored the marketplace and have tested out many cloud based products trying to find those that would start to make more economic sense for the broader market. We have seen the costs of online backup plummet while the reliability has improved greatly, and we have seen a growing acceptance of cloud based email and document storage/access solutions, especially with the explosion of smart phones. And now, we have found the first cloud solution that affordably removes the need to purchase and maintain PCs and servers, removing one of the larger headaches of IT implementations.

Essentially, the Cloud can now eliminate the need for buying computers for each individual employee. Instead, much like any utility service for your business, you are billed monthly for however many PC desktops you use. Instead of a PC, each desk would have a "Receiver" device to which you can hook up all of your desktop items (monitors, keyboards, printers, USB Drives, etc). This Receiver (using 1/3 less electricity than a PC) then connects directly to the Cloud using secure Citrix in order to access the PC desktop. In addition, when away from the office, you can access your desktop and company server securely from your iPad, iPhone, Android phone/tablet, or your home desktop or a laptop (with no need to leave anything on and running overnight in the office). The only requirement being that you have an Internet connection that can handle the basic speed requirements. While Verizon FiOS is recommended because they offer faster upload speeds with less built in delay than the other cable providers, we have found that it does work just fine on user setups using providers like Comcast.

By removing all the PC and Server hardware from the office, a great deal of time and effort can be saved on computer maintenance, and the disruptions of hardware failures can largely become a thing of the past. Even if your desk gets flooded, or stolen by aliens, or crushed by Godzilla, you can simply log in securely from any other cloud Receiver or any other PC/Smartphone/tablet, from any location with Internet access, and your customized desktop, with all your documents, settings and server access, will be there just as you left it.

After reviewing the cost of owning and maintaining a PC by looking at our records over the last decade across all of our clients, we have been able to get a good idea of the yearly actual costs including hardware, software, maintenance, and the average risks of hardware failures (bad hard drives, power supplies, motherboards, memory, etc), and it is now finally within the range of hosting the PCs in the cloud instead. We also believe that cloud hosting will continue to decrease in price over the next few years, making the hosting option more and more attractive as time goes on.

Beyond the costs being close for either in-house, or cloud based PCs/servers; there are the other benefits of moving to the cloud:

- Never need to replace a computer or server
- Backup and anti-virus costs are included
- Securely access your desktop from anywhere
- Greatly reduced technical support costs to maintain equipment
- Highly scalable and easily upgradable
- Greener solution, since it uses less electricity
- Much less hardware that can break, and therefore less downtime during the year.
- Only pay for the users that you have that month, no more paying for that PC that sits unused in the corner, growing obsolete.
- Easier to budget costs... no more "surprise, you need to buy 3 more desktops this week for thousands of dollars you hadn't planned on."

So finally we feel there is a comprehensive cloud solution where the performance and costs are in a reasonable range, and the benefits make sense for a lot of our clients. However this solution is not for everyone and there are some requirements (mainly good Internet access) that would need to be met. So if you never want to pay upfront and maintain the hardware of a computer or server again or are interested in moving your company to the cloud in some form, please call us at 866-9MH-TECH (964-8324) or email info@mhconsults.com and one of our technicians will be happy to answer your questions.

Issue 36

February 2012

Page 2 of 2

THE M&H MONITOR

M&H CONSULTING

Wireless Network Security

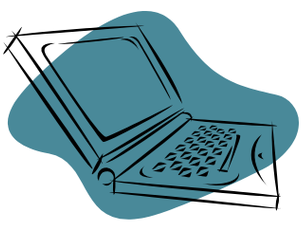
Scott McDonald

In recent years, wireless networking has become more and more popular. Laptop computers, smart phones, and tablet devices all have become essential business tools, and integrating these devices into your business office usually requires a wireless network. While many of these devices come with 3G and 4G data plans available, the speed and security of these networks cannot match what is provided with a properly configured wireless local network.

So you already have a wireless network set up in your office or at home? Great! The next important step is making sure that it is secure. If your wireless network is not properly secured, it can be broken into by even the least skilled hacker who is willing to do a little research.

Some people may not care if others use their wireless internet however they should keep in mind, surfing the net might NOT be what they have in mind. If someone with basic networking skill accesses the network, the hacker will be able to scan all of the devices and computers attached to the network, and potentially gain access to the data stored on them. What's worse, the company would probably never know that the intrusion occurred. They could also be held accountable for actions taken by a hacker while using the Internet connection.

Some may say that they already have security on their wireless router however, if they purchased and set up a wireless



router themselves, or if it was set up by their Internet provider, there's a chance the network is not very secure. The router could be using an outdated type of encryption, or no encryption at all. On most wireless routers, the default security setting is to use WEP ("Wired Equivalency Protection") encryption. WEP uses an algorithm to encrypt ('scramble') the contents of all information being passed over the air, so that only the router and a computer with a manually entered "key" can decrypt it. Unfortunately, WEP encryption has been hackable for many years, and today it is easy to find tutorials and tools online for hacking WEP. WEP is still included in routers because it is universal, and older wireless devices may need to use it.

In order to use the best security users should ensure that their router is using the most current type of encryption, if possible. Most recent laptops and wireless devices can use WPA2 encryption. They should also consider changing their network passphrase periodically, and change it immediately if they suspect unauthorized access. Another step to minimize exposure is to turn off "SSID broadcasting," which simply means that your router will no longer announce to the world that its wireless network is available. This way, a user would have to already know that the network exists, and would need to know the name of it in order to even attempt logging in. Keep in mind that any changes made to the router would need to be configured on each device that accesses the network.

If you have questions about securing your wireless network, you can call M&H Consulting at (866)964-8324 or email support@mhconsults.com.

TAKE $$$CASH$$$ FROM M&H CONSULTING

Refer a new Tech-For-A-Day client to M&H Consulting and mention this offer to us, and you will receive $25 for each PC the new client has. Call for details.