Issue 44

January 2015

Page 1 of 2

M & H CONSULTING

THE M&H MONITOR

Backing Up Your Data!

Justin Bowden

When it comes to our clients business, one of the most important things that they have is their data. Ensuring that this data is always available is usually priority number one in the IT world. There are many different ways that you can backup this data and ultimately the decision is based on the individual business needs. There are two main types of backups, local and Cloud, each with their advantages and disadvantages.

The first type, and the most common currently, is local backups. A local backup needs the following items to work. First you must have some sort of backup software, such as Backup Exec from Symantec. Next you must have somewhere to back this data up to. This could be an external tape drive, an external hard drive, or another computer or server. Once you have those you create a backup strategy. This would include how often you will be rotating your media, what you will keep onsite vs taking off site, what types of backups you want to run (full or incremental).

The advantages of local backups include the following: **1) Peace of mind** – Your data is generally as protected as your network. Once you disconnect the media it usually is safe from malicious attacks. **2) Speed** – Generally local backups are quicker. **3) Control** – You control where this data is, who can and cannot access it.

Some of the disadvantages include: **1) Cost** – Generally local backups cost more than their cloud counterparts. **2) Flexibility** – If you need to increase your storage space you will need to add additional tapes or hard drives. **3) Disaster Recover** – If backup is kept onsite you could risk losing access to it in the case of a disaster on site.

The second type of backup is Cloud based. Cloud based backup requires a subscription or purchased storage space with a cloud based backup provider. After that it is just a matter of setting up the backup job.

Some of the advantages of cloud based backups include: **1) Cost** – Generally it costs much less to back up the same amount of data on the cloud as you would with a local backup. **2) Accessibility** – Because you can access your data from the internet you can recover data on the go. **3) Flexibility** – With cloud backup if you need more space usually it only take a few minutes to increase your plan. **4) Disaster recovery** – In the event of a disaster on site you don't need to worry about data not being accessible.

Some of the disadvantages include: **1) Speed** – Because you are backing up over the internet the speed is going to be limited to your network and bandwidth. **2) Security** – While this has become less of a factor, no data that travels over the internet will be 100% safe from hackers or malware. **3) Control** – If you have highly sensitive data, an inability to retain full control over storage process may be a drawback.

While there are many choices that business owners need to make about their backup they need to be aware that ultimately there is no one best backup strategy, but will depend on the needs of the business.

One final piece of advice. If your company has a server, it may be prudent to ensure that you have a second backup server in place. This may be an added expense now, but could ultimately save thousands if your single server happens to crash. If you have any questions about backup strategies or need a backup plan setup please contact us at **866-9MH-Tech** or

support@mhconsults.com

General Troubleshooting Tips to Keep In Mind

There are many different things that could cause a problem with your computer. No matter what's causing the issue, troubleshooting will always be a process of **trial and error**—in some cases, you may need to use several different approaches before you can find a solution; other problems may be easy to fix. We recommend starting by using the following tips.

- **Write down your steps**: Once you start troubleshooting, you may want to **write down** each step you take. This way, you'll be able to remember exactly what you've done and can avoid repeating the same mistakes.
- **Take notes about error messages**: If your computer gives you an **error message**, be sure to write down as much information as possible.
- **Always check the cables**: If you're having trouble with a specific piece of computer **hardware**, such as your monitor or keyboard check the cable connections.
- **Restart the computer**: When all else fails, one of the best things to try is to **restart the computer**.

Issue 44

January 2015

Page 2 of 2

THE M&H MONITOR

M & H CONSULTING

Keeping You and Your Devices Safe

Justin Bowden

In today's fast paced world we are becoming more and more dependent on our electronic devices. We access our data and spreadsheets on our laptops and tablets. We call and email our clients on our smart phones. The devices we use are becoming more integrated with everyday life, and as such we use them for more than just business.

Many people will stream a video, or listen to music on their devices. Imagine, however, you click on a link to watch a video, and instead your device becomes locked, with a message stating that there is child pornography on your device and you will be reported to the FBI unless you pay to have it removed. This is exactly what happened to a young girl in Tennessee. She unknowingly installed malware that took over her phone and started to wreak havoc.

This type of malware is called "Ransomware". It is a form of malware that installs on your devices, and can be from websites, emails, etc. Some of it will threaten to delete or encrypt your data unless you pay a fee. Some will delete the data and then demand a fee to restore it. Some, like above, will install illegal things and demand that you pay or if not that you will be reported to the FBI. What's worse is that you could pay the ransom demanded, and you're not even guaranteed to get your data back, or device freed.

This type of malware is big business, and has mostly been limited to computers (laptops or desktops.) With today's technology of more mobile devices such as tablets and smart phones we can expect that this will become the newest trending market for being targeted by the writers of the Malware. Companies such as Avast have reported in increase of blocked attacks, and they see the trend rising.

All hope is not lost however. There are steps that you can take that can help you to avoid this type of personal attack. First you should always be wary of links. Never click on an unknown link, especially from emails. If an associate or friend has emailed you something that contains a link make sure that you verify that it actually came from them before clicking on it. Attackers have ways of making emails seem to come from people you know and wouldn't suspect. Second, you should only use approved methods of downloading applications onto your smart phone or tablet. This includes Google Play and the Apple Store. This is not always a guarantee of safe programs, but they are less likely to be harmful if coming from them. Third, make sure that you have some sort of program to block these types of attacks. This means virus/malware protection. Make sure that you use a reputable vendor, and purchase the protection. There are many free versions out there, but when it comes to your devices and data it is better to be safe than sorry. You know the adage, you get what you pay for.

If you do become the victim of one of these ransomware attacks make sure that you first contact your local authorities, especially if the ransomware has downloaded illegal items onto your device. After that you can contact us any time at **866-9MH-TECH** or email us at **support@mhconsults.com** and we will be glad to assist you.

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.