Disaster Recovery: The Most Critical Part to Data Backups That Most Companies Overlook

"As a business owner , I know you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems forever."

Joe Stoll, President
Technical Action Group (TAG)
JStoll@TechnicalActionGroup.com

Inside this issue:

You'll recall a few months back tornados ripped through Joplin, MO and Tuscaloosa, Alabama causing massive devastation. The fortunate ones only had to suffer through minor interruptions of utility services, with others paying a far steeper price.

In fact, a fellow member of my Managed Service Providers master mind group that meets in Nashville on a quarterly basis had his office in Joplin reduced to a pile of rubble. That was his office in the photo. Thankfully as a computer support provider he practiced what he preached and was prepared for such a disaster. While he endured the inherent difficulties in rebuilding, he had a disaster recovery solution in place that allowed him to resume business from another location in 36 hours, and continue to service those of his clients that had the same recovery plans in place.

This is a perfect reminder and excuse for me to harp (as I'm known to do on this topic) about the importance of disaster recovery planning to any business. Sure, as Canadians we don't face risk from tornadoes and hurricanes (though hurricanes are becoming more common outside of Toronto), but we are not immune from the destruction caused by fire, flood, theft, and employee error—any of which can shut your doors without a proper recovery plan in place.

No one expects terrible things to happen, but when they do, having that plan in place can really save your bacon. And one of the MOST important aspects of this is the *recovery* part – how are you going to get that data back onto a working platform that allows you to continue serving your customers and operating your business. <u>The shocker for most business owners is that simply having a copy of the data does NOT guarantee a fast recovery</u>. Let me give you an analogy to help you understand…

Let's suppose we put a disaster recovery plan for your home. Your house would represent the server and platform, and all your furniture and personal items would be the data. Now let's suppose we could make a backup of your home by making an exact copy of everything that's in your house (all your furniture, appliances, clothing, etc.) and storing it in a "backup" shed. Then the unthinkable happens: your house gets leveled by fire or destroyed by flood and everything is gone (or a critical part of it is damaged and needs to be replaced). Or all your contents are stolen. You would think, "Well, at least I have a copy!" True, but the first thing you would need to do is replace the home itself (remember, that's the platform that everything resides on).

Next you would have to "reinstall" the services like gas, electricity and water (let's call that the software). Then you would have to haul everything from the shed back to the house and "reformat" it by arranging it into the house. Depending on the extent of the damage done to your house, that could take days or weeks; chances are you'd have to find a hotel to live out of in the meantime. In addition, there's the time and cost of moving everything back in and re-arranging and restoring everything to its proper place.

Shiny New Gadget of the Month:
Bedphones

Just like when you were a baby, you just can't seem to drift off to sleep without a lullaby. While your lullaby preferences may have changed from songs like "Rock-a-bye-baby" or "Hush Little Baby" to tunes by U2 or perhaps the latest *Idol* winner, the need for soothing still exists. And most likely you have been forced to go to sleep with standard headphones that cause a bit of discomfort.

Well not anymore!

Bedphones have cushy pads and ear-hook style buds that are extremely thin and held in place by a length of moldable memory wire.

They also come with an app available on the Android platform that can shut off the music automatically when you fall asleep. There's also the ability to set a timer which gradually counts down music volume as the timer runs down.

Soothing music and comfort all in one! Get your Bedphones for about $30.

Learn more at:
store-
4cf2b.mybigcommerce.com

Plus, the above *assumes* you have a recent, working copy of your entire home and everything in it. If you failed to make a copy – or if the shed where you were storing everything had a water leak that destroyed everything inside due to mold – then you're really out of luck.

Of course, this is a simple analogy – and there are ways to back up your data and network so that recovery can happen inexpensively in a matter of hours versus days or weeks. But if you simply think having a tape backup is going to be your saving grace, you might be unpleasantly surprised. I can't tell you the number of businesses who ended up losing incredibly valuable, irreplaceable data because they didn't think through the RECOVERY part of the backup equation.

So what do you need to think about? First, the way you backup your data should be based on how important your data is and how fast you would need to be back up and running in the event of a disaster. If losing your data would only be a mild inconvenience and you could stand to be down for a couple of days, then tape backups may be okay. If that's not an option for you and there are certain critical functions that need to happen to keep you from getting into hot water with your customers and to prevent you losing a LOT of cash, then you want something more reliable than tape drives.

The BEST thing to do is contact Joe Stoll at our office at JStoll@TechnicalActionGroup.com or 416-489-6312 x 204 to schedule a free, no –obligation strategy meeting to go over your needs and expectations for what should happen in the event of downtime or an outright disaster. That way you know for sure what to expect and – more importantly – how to accurately prepare for a disaster—since Dilbert's plan isn't very effective.

How To Keep Your Laptop Secure When Using Wi-Fi

You can't beat the convenience of checking e-mail and hopping on the Internet at (Wi-Fi) hotspots found in airports, coffee shops, bookstores, and even in some major parks. For the uninitiated, Wi-Fi hotspots are areas where you can use your wireless laptop to surf the Web and check e-mail. But the question you have to ask yourself is, just how safe is it to connect? With the proliferation of hackers, viruses and identity theft at an all time high, you are smart to be concerned. Wi-Fi spots are very attractive to hackers because they can use what's called an "evil twin" connection to access your laptop.

An evil twin is a wireless hotspot set up by a hacker to lure people from a nearby, legitimate hotspot. For example, when you log in at your favorite coffee shop, you might actually be logging onto the evil twin Internet connection set up by the innocent-looking person working on a laptop at the next table.

The most dangerous evil twins remain invisible and allow you to do business as usual. But in the background, they record everything you are typing. Buy something online and they are recording your credit card information. Log on to your bank account, and they can grab your password. Some hotspots may even feed you a fake Web page after you log on asking you to update your billing information. This is the same tactic used in phishing scams.

So what can you do to make sure you are not giving an evil twin access to your laptop? First, know the name of the hotspot by asking someone who works there. Some businesses will give you printed instructions that include the hotspot name. Again, be careful. Hackers will try to name their evil twin network by a very similar name as the real hotspot, and may even show up as a stronger signal.

The best protection you can have is connecting via your company's VPN (virtual private network). A VPN will protect your online information by encrypting your data and activity even if you're connected through an evil twin. If you don't have a company VPN, you should assume that someone is looking over your shoulder and recording everything you type in. The BEST protection without a VPN is to never type in information such as credit cards, passwords, or social insurance numbers when connected to a public Wi-Fi hotspot.

If Getting E-Mail Anytime, Anywhere, On Any Device WITHOUT Any Downtime Is Critical To Your Business, Read On...

Is e-mail communication the lifeline of your business? Would your productivity grind to a halt if your e-mail was cut off for any time at all? Are you tired of new hardware and software expenses and the endless maintenance needed just to keep everything up to date? If so, I've got some great news for you.

Cloud Based E-mail (aka "Hosted Exchange") is often a much easier way of eliminating e-mail downtime, slow performance and annoying spam messages. Here's how it works: Instead of purchasing and maintaining your e-mail in-house, which can be costly and time consuming, your e-mail server is hosted (and maintained) in a high-performance, high-security hosting company "in the cloud" where you can access it securely from any device or PC.

Best of all, you don't have to make any changes in HOW you access your e-mail – your messages will simply be delivered to your inbox, phone or other device faster and with fewer issues, and it will always be synchronized and up-to-date!

Here are just a few of the advantages of cloud-based e-mail:

⇒ **Synchronized access to your e-mail and calendar from anywhere.** You don't have to remote into your office PC; now you can securely access your e-mail from any device or PC.

⇒ **No more software, hardware or maintenance costs.** YOU don't have to purchase the hardware and software, nor do you have to maintain the system. This is all included in a very low monthly fee.

⇒ **High speed, "always on" e-mail.** The hosted Exchange platforms we provide to our clients are high-performance systems with multiple "fail over" backup servers, maintained and monitored like Fort Knox, which is a level of service you wouldn't typically need for your small business. However, since you are hosting on this platform, cloud-based e-mail gives you all the benefits of a high-performance system without the costs. Your in-house network could go down and you'd STILL have access to your e-mail, contacts and calendar.

⇒ **Automatic backups and archiving.** What would you do if your in-house e-mail server failed and erased your messages? Or what if a disgruntled employee deleted all their e-mails? If you were hosting your Exchange, these would be non-issues since your e-mails are backed up daily and secured.

How To Get Rid Of All Your E-mail Problems, Finally And Forever!

Want to know if Cloud-Based E-mail is right for you? Call us for a no obligation, no pressure "Cloud E-mail Readiness Assessment." We'll show you how much it will save your company in hardware, software and support costs, and we'll let you know if there are any hidden "gotchas" to consider for your business. If you decide to switch your e-mail to a hosted solution with us (and you are under no obligation), we'll even waive the setup fee.

Call Joseph Stoll today: 416-489-6312 x 204
Or e-mail: JStoll@TechnicalActionGroup.com

---

lse

.com

9 Steps You Must Know To Prevent A Server Crash

Here are a few simple things you can do to prevent your server and network equipment from overheating and crashing:

- Tidy up the server room; a neater room will increase air flow.

- If you have more than one server, arrange them in a row so that the cold air comes from the front and is expelled out the back.

- Keep the doors to the server room closed and seal off the space.

- Make sure cold air reaches all the equipment.

- Have a redundant A/C that is specifically designed for computers.

- Buy a rack enclosure where the cooling is built in to the bottom of the rack.

- Keep the temperature at no more than 77 degrees.

- Use blanking panels over any empty spaces on your server rack.

- Consider virtualization or hosting in a cloud environment so you are generating a lower amount of heat in the first place.

7 Reasons Computers Run Slower As They Get Older

Do any computers in your office run so slow so as to drive you or your employees blood pressure to rise? Do any frequently freeze up, crash and take forever to open files? Aside from the obvious frustration and reduced productivity slow computers cause, it may actually be due to one or more of the following:

Slower boot due to installed software. To increase your security, software such as firewalls and antivirus applications must start up immediately when you boot up your PC. This of course will cause it to start up slower. Some software partially loads at boot so when you launch applications they seem to start faster. Plus, device drivers and helper software for printers, multimedia devices, and other peripherals may require being loaded at boot to make using such devices in a plug-and-play environment as seamless as possible. All of this increases your overall boot time.

Slower overall experience due to installed software. Just as loading applications slow your computer's boot time, they also may require additional CPU cycles, causing your main applications such as web browsers or word processors to run slower. Plus, more tasks consume additional RAM, requiring your computer to use your hard drive as virtual memory. Paging information to and from your hard drive increases the disk thrashing, slowing down your computer further. You can help offset this somewhat by installing additional RAM if supported by your computer.

Uninstall software doesn't always work well. While most applications support an uninstall procedure, these don't always work perfectly. Uninstallers may leave temporary files, items in the Windows Registry, startup tasks to files that no longer exist,, device drivers that now are not needed, etc. Install and uninstall many applications and the leftover garbage can drastically slow your computer's overall speed if the garbage isn't tossed out.

Unneccessary Programs. Many PCs come with programs automatically installed to run at startup. Over time, these programs (along with all the other programs you install) can significantly slow down your computer. They are often running in the background, but are never used.

Updates require more power. Updates to your device drivers, software, and operating system just may require more computing power than older versions. This can be due to sloppy programming or the addition of newer features. Plus, as security holes are fixed and workarounds created, such software may require more CPU cycles, RAM, and overall storage space on your hard drive. Security is one reason why an older version of Windows may run much faster than a newer version. While the older version may seem to work fine, its lack of protection features can expose your computer to all types of security risks.

File fragmentation. Over time, the files on your hard drive get broken into pieces when saved, which causes your operating system to take more time to find, open and update files. To prevent this, your hard drive should be defragged on a regular basis.

The dreaded malware. Of course, viruses, spyware and other malware may be to blame. These create additional processes that put more strain on a computer and can increase its overall boot time. Other users may be lurking around your PC via an open port, causing all sorts of chaos. Malware may be running in the background using your computer to relay e-mail messages, attempt to shut down websites via denial of service (DoS) attacks, and more. So though security software may adversely effect your computer's overall speed slightly, not having such software (and keeping it updated) can cause an even worse situation.