Bits & Bytes

Insider Tips On How To Use Technology To Make Your Business Run Faster, Easier, And More Profitably

Technical Action Group Inc
TAG we're I.T.

"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:

Volume III, Issue VIII **August, 2011**

4 Questions About Backups That Business Owners Should Know The Answers To

The old saying, "Pack your own parachute," comes to mind when I think of data backups or, more specifically, data RECOVERY. However, how many people actually know how to pack their proverbial data backup "parachute" and instead rely on someone else – be it an employee or vendor?

If that's you, read on. Since the absolute WORSE time to check your backups is AFTER a data disaster, all company CEOs ought to know the answers to the following questions NOW so they aren't unpleasantly surprised later when data gets erased and they're scrambling to get back up and running:

1. **Where EXACTLY is your data being backed up, and how do you get access to it?** If it's being hosted in a remote place, you ought to have the account information and a direct contact you can call if your vendor or employee goes missing with this information. Ideally, it should be in your network documentation that is kept in your operations manual or somewhere you can easily access it if necessary.

2. **Who's responsible for monitoring the backups to make sure they are working?** When data is lost, the finger pointing starts. It's not uncommon to hear, "Well I thought (they/he/she) was in charge of our backups!" only to discover that this person (be it a vendor or employee) actually has no idea that they had such an important responsibility. Keep in mind that many offsite backup companies allow you to store your data there, but they won't agree to ANY responsibility for whether or not the data is being backed up correctly, completely or in a format that can be restored.

3. **How often do you run a test restore?** The only way to know if your backups are working properly is to conduct a test restore or "fire drill" of your data. We recommend this be done once per month at a minimum to verify that you can actually restore from your backups in an emergency.

4. **If your data is lost, what's the process required to restore it?** Some business owners don't realize that their raw data backups would take a LOT longer to restore than they imagine. If you are not "imaging" your data (a process that takes a snapshot of your server as is) you will have to reload all of your software, set up the network, reconfigure your settings and THEN restore the data – a process that can take the better part of a week PROVIDED you still have your original software discs and licenses.

Our Free Backup Audit will give you the answers to these critical questions. If you don't know the answers to these questions, give us a call to schedule a FREE inspection of your backup process. At a minimum you'll know for sure that your data is safe and in a format that can get you back up and running again FAST. Call Joe Stoll at 416-489-6312 x 204 or email him at:
JStoll@TechnicalActionGroup.com

Shiny New Gadget of the Month:

EchoSign® You send. They sign. It's done.

If you are a business that is still faxing or mailing documents because you need a signature, you'll love this month's gadget, EchoSign.

Contracts have been faxed and mailed for years because of the binding laws associated with signatures.

EchoSign allows the legal, electronic signing of documents to speed up the signing process – now you can e-mail a PDF, Word document or Excel file to someone and allow them to "sign" without printing it off, signing and scanning, faxing or mailing it back to you.

The free version of EchoSign allows the user 5 signatures a month, which may be adequate for those that only deal with contracts and other signed documents once in a while. However, for those that need to use the product on a daily basis, upgrading to the Pro version costs $14.95/month, the Team version (2-9 users) is $40/month and the Enterprise version for 10 or more users costs $299/month.

In addition to speeding up the signing process, this app also allows you to track, organize and file your paperwork securely online, available for reference at any time.

For those who prefer to keep the paper trail organized in computer files instead of physical files, EchoSign would be a great help.

Can You *Really* Get Microsoft Office For Just $6 A Month?

Recently, Microsoft announced a real "game changer" for the IT industry and something that may mean the demise of the $62 billion-dollar company's stronghold on the desktop. What is it? Office 365, which is their new cloud computing answer to Google Apps. Instead of paying hundreds of dollars per license, you can now access the entire Office suite of products via the Internet for $6 to $24 per month (like paying for a utility).

What Is "Cloud Computing"?

Cloud computing or "going to the cloud" is very similar to the concept of paying for electricity as a utility rather than purchasing and running your own generator to power your home or office. Public utilities can provide a cheap, reliable, "pay as you go" service to anyone wanting water or power. Similarly, cloud computing means that the cost of hosting, securing and delivering services (like Office) is owned by the utility company (in this case, Microsoft).

Is This A Smart Move?

The cost savings with Office 365 are hard to ignore; however, there are a number of things to consider before you jump ship to cloud computing. You need to consider the reliability of your Internet connection, what type of help desk support you want, security, what other applications (accounting, CRM, line of business applications, etc.) you need and which devices (scanners, printers, iPads) you need to use. Many people also have concerns about security and where their data is kept (within Canada, USA or offshore) – all things that need to be addressed before you move to the cloud.

Is Slow Access To Your Work Files From Home Driving You and Your Employees Crazy?

Last month while we were getting a new client set up in our monitoring systems, we asked them if any of their staff need to access files on the network from outside the office. Turns out a number of their staff work from home occasionally, and also travel for work. While they were able to access files on the network, they were doing so through VPN which was extremely slow. Staff and management were all frustrated because they weren't productive when they were working away from the office.

As if that wasn't annoying enough, they had to download files before leaving the office and then upload changes to files. Clearly, there's a huge risk that people either forget to do it, or don't upload changes promptly, exposing them to a plethora of mishaps from having outdated files on their main server.

Our client needed to provide additional staff with the flexibility to work from outside the offices; however were concerned about increasing the low productivity and exposure to errors with each new person, if a better solution wasn't found.

TAG recommended installation of a Windows Terminal Server. This server contains all company files and serves as a secure access point for staff to work from and access and update data stored inside the network. Now staff can work away from the office just as if they are working inside the office, connected to the main server. Our client also has the peace of mind knowing that even though their staff can access files from outside of the office, no one else can as Terminal Server is far more secure than VPN.

Do You or Your Staff Need A Secure, Flexible Option to Work from Home? Call Joe Stoll Today at 416-489-6312 x 204 for a Free Evaluation!

A Simple, Very Affordable Way To Increase Employee Efficiency (and Yours!) By 25%

According to a University of Utah study, you can increase your efficiency (or your employees' efficiency) by 25% just by adding a second monitor. With multiple monitors, you can get more done since you aren't minimizing and maximizing all day long. Therefore, adding monitors can be a money maker for your company.

The study documentation states that 108 university and non-university personnel participated in a comparison of single monitor, multi-monitor, and multi-monitor with Hydravision display configurations. Respondents edited slide shows, spreadsheets, and text documents in a simulation of office work, using each of the display arrays. Performance measures—including task time, editing time, number of edits completed, and number of errors made, as well as usability measures evaluating effectiveness, comfort, learning ease, time to productivity, quickness of recovery from mistakes, ease of task tracking, ability to maintain task focus, and ease of movement among sources—were combined into an overall evaluation of productivity. Multi-screens scored significantly higher on every measure. Respondents got on task quicker, did the work faster, and got more of the work done with fewer errors in multi-screen configurations than with a single screen.

Consider trying this in your office. Add a monitor or two to your desk and to those of your employees. See what kind of feedback you get and how much more efficient and productive they become when they have the ability to move quicker, use multiple applications at once and no longer have to constantly minimize windows.

The good news is that monitors have really come down in price over the years. You can get a 19 or 21 inch for between $175 and $300. A small price to pay for the productivity payoff.

Most of us at TAG have been working with dual monitors for the past many months and the positive effect on productivity was instant! They are so thrilled with how it's made their jobs so much easier and quicker, we couldn't buy these monitors back from our employees if we offered them triple what we paid for them!

Should You Leave Your Computer On At Night or Shut It Off?

I am often asked by clients and colleagues whether or not they should leave their computer on all the time or turn it off when they are not using it. Several years ago I would have told my clients to turn their machines off to save power. But with the proliferation of viruses and threats over the last few years, I have changed my mind.

Today, anti-virus programs and anti-spyware applications need regular updating. These updates are often scheduled to run in the wee hours of the morning when you are not using your computer.

Windows also needs to be updated whenever a new security patch is released. This is usually not daily, but it may happen several times a month. It's important to update your operating system as soon as a patch becomes available because hackers move very quickly to reverse engineer Windows updates. As soon as an update is released, they create a virus specific to that vulnerability and start looking for unprotected machines to infect and invade. So bottom line, leave your computer on all night and restart it two or three times a week to clear the memory.

Tools to Drive Productivity Using Your Smartphone

New apps are constantly emerging for iPhone, BlackBerry, Palm webOS, Windows Mobile and Android that help boost productivity in business. I've listed 2 of them here. Check back next month for more!

App: Gwabbit

Why You Need It:
Gwabbit's patent-pending semantic technology simplifies contact capture & management, automatically scanning incoming e-mails and transforming sender information into contact records in your address book.

Features:
Address book management prompts, alert services for contacts who've been "gwabbed"

Available For:
Blackberry

Price:
FREE

App: Inventory Tracker

Why You Need It:
Forget spreadsheets. With Inventory Tracker, stay on top of what products you have for sale, what's already sold and what needs to ship. And if you don't want to forget spreadsheets, the app exports your inventory data to Excel, too.

Features:
Real time updates, cost calculator.

Available For:
iPhone

Price:
$4.99

Chew Gum And 3 Other Simple Ways To Prevent Heart Disease

In addition to avoiding the "big" things like smoking, obesity and high cholesterol, there are a few small things you can do to impact your cardiovascular health:

Take two baby aspirin daily. The American Journal of Medicine concluded that taking 2 baby aspirin a-day can reduce the risk of a first -time heart attack or stroke by 30%.

Chew gum and floss. People with gum disease are three times more likely to have a heart attack than those without it. That's because plaque, the sticky film on your teeth, harbor bacteria. That bacteria then enters the bloodstream and causes chronic inflammation that increases the risk for clots and other heart attack risk factors.

Drink tea. A heart specialists at Brigham's Women's hospital discovered that people who drank one or more cups of black tea daily were 44% less likely to have a heart attack than those who didn't drink tea.

Take a Vitamin D supplement. Vitamin D is considered the "hot" new supplement for good reason; it's considered that two thirds of all Americans don't get enough of the critical vitamin. In addition to an increased risk for heart disease, vitamin D deficiency is also linked with insulin resistance, metabolic syndrome, hypertension and diabetes.

You Just Discovered An Employee Had Their Laptop Stolen or They Lost It—Quick—What Do You Do?

I've come across some alarming statistics that you should know. There are 12,000 or so laptops found in US airports each week and 62,000 lost electronic devices recovered from New York's metropolitan buses, taxis, trains, and stations each year! I couldn't locate the statistics for Canada, but it's a safe bet the numbers are equally frightening. The bottom line is no matter how careful you are with your laptop, mistakes occur and losing a laptop (or having one stolen) is likely to happen to you or your employees at some point in time.

In the hands of a relatively unsophisticated hacker, all of your laptop information can be siphoned off, allowing an open back door into your network. This is akin to giving a thief the key to your office and the code to deactivate the alarm. Imagine the embarrassment of having to contact all of your customers to let them know THEIR confidential information may be compromised because one of YOUR unsecured laptops is in the hands of a criminal!

Asking employees to be more careful about where they keep their laptop IS a good step in the right direction, but accidents happen and thieves are always on the prowl. That's why it's so important to take measures to lock down and secure any mobile devices you and your staff use to access your company's network. Here are just a few things:

Encrypt All Information – Drive encryption software such as BitLocker (which is included in some versions of Windows 7) can secure all the data on your hard drive. Also, check your computer to see if it has a Trusted Platform Module (TPM) chip which is generally more secure than those without TPM.

Multi-Level Access Security – Don't rely only on passwords to keep your laptop safe. Hackers can usually break most passwords in a few hours. We recommend adding a second way for people to prove that they are who they say they are BEFORE they are able to log in. Some people use smart cards to do this, but fingerprint pads are gaining in popularity.

Log / Back-Up Information – It's critical to log and back-up all information on business laptops to ensure smooth operations in the event of loss or destruction. We can automate the backups so they are done ON SCHEDULE and in a way that won't interfere with the use of the laptop.

The Right Response - What happens when an employee loses a laptop? Do you have a next step action plan? If not, we suggest calling us (or your IT provider) immediately to report the loss. The sooner we / they know, the sooner preventative action can take place to lock that laptop out of the network. A blame culture where people are afraid to report losses is very bad for security.

How to Avoid Online Viruses When Surfing The Internet

You can't operate a business these days without online access – but hackers and cyber criminals work around the clock to find new ways to infect your computer and access confidential information. What makes this even worse is the fact that many viruses are introduced unknowingly by the user! To avoid downloading a virus to your PC, here are a few simple tips:

- Keep Your Anti-Virus Up To Date: Every anti-virus software has an automatic update feature – make sure yours is turned "on."
- Never Download Files From File-Sharing Web Sites: Web sites like KaZaa are breeding grounds for viruses. Never download anything from these sites, period! Especially free software!
- Never Open Attachments In E-mail From Unknown Sources: When in doubt, delete the file.
- Never Download Emoticon Programs, Screen Savers, Or Other "Cute" Program Files. Hackers love to use "eye candy" programs like cool screen savers to get users to download their viruses.