ISSUE 7-9

BITS & BYTES

INSIDER TIPS ON HOW TO USE TECHNOLOGY TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY

IN THIS ISSUE

September 2016

"TAG specializes in providing management level responsibility for all the technology in your business. This includes support for your network and working with other hardware & software vendors who's technology you use.

We do this with friendly, proactive & responsive service!

Joe Stoll, President
Technical Action Group (TAG)

Betting The Farm Your Backups Are Safe?

It's only natural that when you hear of a disaster you think it couldn't happen to you.

That's why, even though many businesses are told constantly (especially by us) that they should diligently maintain a working backup recovery system because all your company's data could be lost in an instant, tend to brush off the advice.

Yet disasters do happen when you least expect them, and they can happen to anyone. So to illustrate the importance of staying on top of your data recovery system, here are three tales of "data gone wrong." After all, there's nothing quite like a good horror story to inspire action!

Toy Story 2: Gone!

One morning in 1998, the animators at Pixar Studios working on Toy Story 2 noticed that Woody's hat started disappearing. Then his boots… Then all of Woody – gone! Other characters started disappearing too. A rogue command in their system had started wiping out data. No problem, the team thought, as they pulled out the backups. Unfortunately, the backups were bad and only had data from 10 months ago.

Luckily, one of the project leaders who'd just had a baby had recently asked to have

So they drove to her house and escorted her computer back to the studios "like an Egyptian Pharoah." And as we now know, Toy Story 2 was saved.

Moral:

It's not enough to simply run backups. You need to periodically check to make sure the data is actually getting backed up and nothing is corrupted.

46,000 Insurance Customer Records: Lost!

In 2010, Zurich Insurance announced it had lost a backup tape containing confidential data from 46,000 customer records as it was being transferred from one site to another. To make matters worse, it was later revealed that it took a full year for their headquarters to learn that the tape was missing.

While there was no evidence that the data had fallen into the wrong hands, it was not encrypted and therefore easily accessible by anyone in possession of the tape. The company was slapped with a £2.3 million fine from the British Financial Services Authority.

Moral: If your backups are physical, make sure they're transported and stored securely in a location away from your computer. And regardless of whether your backups are physical or in the

Shiny New Gadget Of The Month:

A Great Night's Sleep In The Palm Of Your Hand

The techno-geeks over at Hello Inc. have just released Sense, a device that helps you wake up feeling great. A tad smaller than a baseball, this little sphere sits on your nightstand next to your bed and monitors conditions in your room while you sleep.

Things like temperature, humidity, light and sound in your bedroom are tracked, along with your body's slightest movements as you sleep. It pairs with your smartphone so you can see patterns and change conditions in your room to get the best night's sleep possible.

Sense can play any number of soothing sounds to help you drift off to sleep. Then, when it's time to rise and shine, it gently wakes you up at the best time in your sleep cycle.

It's priced at $129, and you can find it at hello.is and other online retailers.

cloud or both, make sure they are encrypted with high-level security.

Why MegaPetCo Closed Their Doors

The fast-growing set of chain stores MegaPetCo in the US had refused to upgrade their IT system to one that could handle their needs. One day a systems developer accidentally programmed a query that wiped out their entire database. All of a sudden, operations ground to a halt; from sales to payroll to purchasing and reporting, everything had been tied into that one database. And no backup.

They tried to sue their ISP, but between recommendations to upgrade and failure to do so, the lawsuit was dropped. Three months later, MegaPetCo filed for bankruptcy.

Moral: Backups may seem like a low priority, or even an unnecessary expense. Yet surely there is data that if lost would cost your company dearly. And when you compare the cost of replacement to the relatively minor expense of keeping good backups, the choice is clear.

Why Take A Chance That Your Backups Are Safe?
Our FREE Data Recovery Audit Will Help You Know For Sure!

The effects of a data disaster run the gamut from minor annoyance to a death knell for the organization it happens to. We don't want that for you. That's why we're offering our complete audit, normally valued at $395, free to our readers of this newsletter in the GTA.

At no charge, a data security specialist will come on-site and audit your current data backup and security procedures and determine whether your current system can guarantee you a fast, safe and full recovery of your data.

Depending on what we find, we'll either give you a clean bill of health or reveal gaps in your data backup system that could prove catastrophic. Then, if appropriate, we'll provide you with an action plan for further securing your data with our TAGuard Backup and Disaster Recovery Plan—.But there will be ZERO pressure to buy from us—honestly. We just feel so passionately that ALL businesses should be aware of any loopholes in their backup system, and know how to fix them.

Call Joe Stoll at 416-489-6312 x 204 or e-mail JStoll@TechnicalActionGroup.com TODAY and let's make sure your company isn't betting the farm on a flawed recovery system.

Free Report Download: Critical Facts Every Business Must Know About Protecting And Preserving Their Company's Critical Data and Computer Systems

PROTECT YOUR DATA

"12 Little-Known Facts Every Business Owner Must Know About Data Backup, Security And Disaster Recovery"

Discover What Most IT Consultants Don't Know Or Won't Tell You About Backing Up Your Data And Recovering It After A Disaster

You Will Learn:

1) The only way to know for SURE your data can be recovered if lost, corrupted or deleted—yet fewer than 10% of businesses have this in place.
2) 7 critical characteristics you should absolutely demand from any off-site backup service.
3) Where many backups fail and give you a false sense of security.
4) The #1 cause of data loss that businesses don't even think about until their data is erased.

Claim Your FREE Copy Today at:
http://www.technicalactiongroup.ca/DataBackupReport/

9 Essential Cybersecurity Phrases You Should Know

As with all technology, trendy phrases come and go with the passing of every IT conference and newly released virus. And when dealing with cybersecurity, keeping up with them all can mean the survival — or demise — of a business. If you're looking for a list of the industry's most relevant terms, you've come to the right place.

Malware

For a long time, the phrase 'computer virus' was misappropriated as a term to define every type of attack that intended to harm or hurt your computers and networks. A virus is actually a specific type of attack, or malware. Whereas a virus is designed to replicate itself, *any* software created for the purpose of destroying or unfairly accessing networks and data should be referred to as a type of malware.

Ransomware

Don't let all the other words ending in 'ware' confuse you; they are all just subcategories of malware. Currently, one of the most popular of these is 'ransomware,' which encrypts valuable data until a ransom is paid for its return.

Intrusion Protection System

There are several ways to safeguard your network from malware, but intrusion protection systems (IPSs) are quickly becoming one of the non-negotiables. IPSs sit inside of your company's firewall and look for suspicious and malicious activity that can be halted *before* it can deploy an exploit or take advantage of a known vulnerability.

Social Engineering

Not all types of malware rely solely on fancy computer programming. While the exact statistics are quite difficult to pin down, experts agree that the majority of attacks require some form of what is called 'social engineering' to be successful. Social engineering is the act of tricking *people*, rather than *computers*, into revealing sensitive or guarded information. Complicated software is totally unnecessary if you can just convince potential victims that you're a security professional who needs their password to secure their account.

Phishing

Despite often relying on face-to-face interactions, social engineering does occasionally employ more technical methods. Phishing is the act of creating an application or website that impersonates a trustworthy, and often well-known business in an attempt to elicit confidential information. Just because you received an email that says it's from the Canada Revenue Agency or your bank doesn't mean it should be taken at face value — always verify the source of any service requesting your sensitive data.

Anti-virus

Anti-virus software is often misunderstood as a way to comprehensively secure your computers and workstations. These applications are just one piece of the cybersecurity puzzle and can only scan the drives on which they are installed for signs of well known malware variants.

Zero-day attacks

Malware is most dangerous when it has been released but not yet discovered by cybersecurity experts. When a vulnerability is found within a piece of software, vendors will release an update to amend the gap in security. However, if cyber attackers release a piece of malware that has never been seen before, and if that malware exploits one of these holes before the vulnerability is addressed, it is called a zero-day attack.

Patch

When software developers discover a security vulnerability in their programming, they usually release a small file to update and 'patch' this gap. Patches are essential to keeping your network secure from the vultures lurking on the internet. By checking for and installing patches as often as possible, you keep your software protected from the latest advances in malware.

Redundant data

When anti-virus software, patches, and intrusion detection fail to keep your information secure, there's only one thing that will: quarantined off-site storage. Duplicating your data offline and storing it somewhere other than your business's workspace ensures that if there is a malware infection, you're equipped with backups.

We aren't just creating a glossary of cyber security terms; every day, we're writing a new chapter to the history of this ever-evolving industry. And no matter what you might think, we are available to impart that knowledge on anyone who comes knocking. Get in touch with us today and find out for yourself.

Reasons to Reboot Your Computer Nightly

If you've been a client of TAG's for a while, odds are you (or someone in your company) has been asked by one of our technicians when was the last time you reboot your computer when you call in with an issue. There are often telltale behaviours with a computer that are caused by it not being shut down for days or weeks on end, which a quick reboot of your computer can often fix.

Turning off your computer at night has an obvious benefit: it saves electricity, which saves you money. Rebooting your computer, on the other hand, has less obvious benefits. Most laptops have the ability to go into sleep mode, which makes it easier to skip rebooting. Even though improved operating systems and more efficient computers have made rebooting less necessary, it still has advantages

Flushes RAM

Your computer's random access memory (RAM) is also known as volatile memory, because it's constantly in flux -- as opposed to solid-state memory, such as your hard drive. Your RAM handles lots of different short-term tasks and data, like running processes and holding program values. Rebooting your computer flushes out all this information, allowing your device to start anew and helping it run faster and more efficiently.

Fixes Small Errors

Many computer users are unaware that when they reboot their computer, it runs diagnostics on itself, automatically fixing minor errors. These errors can range from buggy or glitchy applications to problems with the RAM. This is why you'll often find that when your computer freezes, or has a problem you don't know how to fix, simply restarting resolves the issue.

Stops Memory Leaks

Memory leaks occur when a program doesn't close properly. Every program that runs on your computer uses memory (usually RAM) while it's open. When you close the program, that memory should return to your computer. Outdated, overused or glitchy programs, however, can have memory leaks, which occur when memory isn't returned to the computer. Rebooting your computer each night can help prevent memory leaks from occurring.

And if the above is still too "geek speak" for you, just think of it this way. If you never turned your car off when you drove it home, wouldn't it get pretty tired and worn out and cause all sorts of problems? Computers, like cars, and people, need breaks too. Now if we humans only had a reboot button for ourselves...

Are You Addicted To Your Work?

To find out, rate yourself 1 to 5 on the following statements. Give yourself a 5 for "often" and 1 for "rarely":

a) You think of how to free up more time to work.

b) You spend more time working than initially intended.

c) Your work helps you reduce feelings of guilt, anxiety, helplessness and depression.

d) You get stressed when you can't work.

e) You set aside hobbies, leisure pursuits and exercise in favour of work.

If you averaged 4 to 5, then you may be at least mildly addicted to your work.

Is that a bad thing? Not necessarily.

While your well-being requires a certain amount of balance, having the drive, enthusiasm and energy to achieve impossible goals marks many of the most successful entrepreneurs.

-Forbes