ISSUE 7-5

BITS & BYTES

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

IN THIS ISSUE

May 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)

The Most Shocking Threat To Your Network's Security—That Every Single Business Has Yes, Even You.

What's the biggest threat to your data? Hackers? Viruses? Natural disasters? Fire or Flood? Theft? All good guesses—but there's a bigger threat to small business data security that can leak your information, corrupt data, harm operations, and bring everything to a screeching halt.

Surprisingly, it's your employees.

Here are some ways your employees could be compromising your business's security and what you can do about it.

Human Error

When it comes to your network, human error is the number one reason that data gets deleted or corrupted, systems fail, and viruses get through.
Solution: Expect mistakes and take actions to minimize their impact. For example, having a remote copy of critical files could save the day. It's also important to educate
employees about malicious viruses and malware that could affect your network.

Carelessness

The most well-intended and conscientious employees can sometimes be careless. An example might be an employee that openly displays passwords for all of their user accounts on post-it notes to make it 'easier'
to log in,
Solution: The key to handling carelessness is education and clearly established policies. Without them, employees may not truly understand the threat their actions represent.

Smartphones & Mobile Devices

Employees who use their personal devices for work often get more work done and are able to collaborate or take conference calls outside of the office. Yet these devices can pose a serious threat to your business security.
Solution: Create a BYOD (Bring Your Own Device) policy and set up software to remotely wipe a device in case it is lost or stolen.

Malicious Acts of Revenge

While you can't predict what disgruntled employees are likely to do, you can make it more difficult for them to hurt your business and your reputation.
Solution: Establish user accounts with multiple safeguards so employees aren't in a position to access information they shouldn't have. Next, set up content filtering software to detect in inappropriate sites or altering large amounts of data.

Need help implementing the right safeguards on your network? We'd be glad to lend a hand! Contact Joe Stoll at JStoll@TechnicalActionGroup.com or 416-489-6312 x 1

Shiny New Gadget Of The Month:

Want A Little Music With Your Light?

The next time you replace a lightbulb, you can now pick one that will stream your favourite music and light up your life in your choice of over 16,000 colours, all with a tap on your phone.

In case you haven't noticed, some LED bulbs now include a Bluetooth- or Wi-Fi-controlled speaker. And at least one, the MagicLight® Plus, available on Amazon, also lets you pick a light color to suit your mood.

At anywhere from $15 to $129 or more, these bulbs can add music – and light – throughout your home or office in a matter of minutes, at a fraction of the cost of a wired-in sound system.

How's the sound quality? It depends on the one you select.

And it may not resonate like Carnegie Hall live…but hey, it's a lightbulb – what did you expect?

Missing Just One Of These Could Instantly Open Up Your Computer Network To A Cyber Attack

Welcome to the brave new world of cyber-warfare.

Gone are the days when software patches were just for nifty little feature add-ons or updates.
Today, a software update notice could mean your whole computer network is suddenly at risk. Dangers include data theft, crippling malware attacks and mischief you may not discover for months, or even years…

As with graffiti on your garage door, if you don't pay attention and clamp down on bad behavior, your problems have likely just begun…

And, like those who hire a professional security firm to keep thieves out of the warehouse, thousands of CEOs and business owners are now waking up to the fact that it's absolutely imperative to hire a pro when it comes to securing your data network.

Here's why you need a professional handling this for you:

#1: Speed is of the essence.
"If you didn't update to version 7.32 within seven hours, you should assume you've been hacked." That's what software maker Drupal told millions of its customers around the world last year. It's just one example of what can happen if you don't respond with lightning speed.

Once a security breach has been identified, hackers rush in. On "Day Zero," cyber-crooks around the world go after at-risk targets. You've got to be quick to patch the gap, or else you risk a system compromise.

Unless you have the time, knowledge, experience and tool set to respond instantly, you are far better off leaving this to a professional IT firm you can trust.

#2: It's not just the big boys they're after.
Sure, the top news stories are about the attacks on companies like Target, Home Depot and Sony, yet your business is just as vulnerable, if not moreso.

Chances are, you simply do not have the resources that giant corporations have to manage a data disaster. The statistics bearing this out are shocking: more than 60% of small businesses close their doors following a serious data breach.

The threat is not confined to giant corporations. Small and medium businesses are being attacked every day, and, unfortunately, your business is no exception.

#3: Dealing with data breaches requires specialized knowledge, skill and experience.
Here are just a few of the things a competent data guardian must be able to do to effectively protect your systems:

Review documentation and monitor forums. Sometimes your software vendor doesn't tell the whole story. It's critical to check online forums and other communities to see if anyone else is having issues with the new patch before jumping in with both feet.

Know when to apply a patch immediately and when to wait. Typically, somewhere around 95% of patches work hassle-free. The trick is to spot the 5% that don't — *before* installing them. This requires identifying unique patching requirements, and applying exceptions accordingly. For instance:

Does the patch deal only with a security issue?
Or does it just add new features or fix non-security-related bugs? Obviously, security issues get top priority.

Is the system currently having issues?
If not, and if the patch doesn't address a security issue your system is vulnerable to, it may be better to heed the old adage "If it ain't broke, don't fix it."

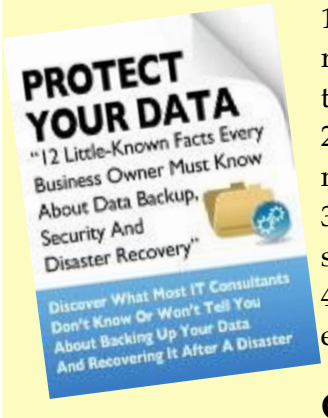
What security gaps does it address?
How severe is the threat to your particular network? If, for example, the only way a virus can enter your system is through an e-mail attachment and this functionality has been disabled for all users, perhaps the threat needn't be a great concern.

Keep options open in case of complications.
Once a patch has been applied, if things aren't working, it's critical to restore the data network to pre-patch functionality, with little if any downtime. That means having good backups in place along with a tested and proven recovery process.

Does just thinking about data security give you a headache? We strongly advise that you let us handle this critical part of your business for you. Call Joe Stoll at 416-489-6312 x 1 or email him at JStoll@TechnicalActionGroup.com and schedule our no-cost Security Update Audit today. You'll discover how easy it is to rest assured that your network is secure 24/7.

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

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
www.TechnicalActionGroup.ca/DataBackupReport

Labrador Retriever Foster #4—Lily!

As lifelong lovers of the breed, Sandra and I were surprised to discover that in fact there are 4 colours of Labrador Retrievers—black, brown, yellow and RED!

Lily came to us after being given up by her family who had enough of her allergies and scratching, and dumped her at the vet.

A kindly vet technician who is very knowledgeable about canine allergies (very common for the lab breed), was sympathetic to Lily's condition, took her home, and within 3 months, reduced Lily's misery by helping her lose 20+ pounds, straighten up her diet, her fur grrow back and she got on the proper allergy meds.

Dealing with a dog with allergies can be an exasperating ordeal (Sandra and I had two of our own), but with enough patience, love and education, it is possible to manage them. Most times it's as simple as changing their diet from dry kibble, to natural raw food.

Lily was with us for a week and was a complete angel. We called her the Red Ninja, for how positively stealth like she navigated her world, and she never made a peep! Lily went to a great home with a married couple who, after years of a gregarious lab, were looking forward to a more calm canine companion—Lily was a perfect match!

http://www.lab-rescue.ca/

The 5 Biggest Mistakes All Leaders Make

Although everyone agrees that hiring is tough, most managers struggle with an even more prevalent leadership mistake. It's an affliction as prevalent as the common cold, and one of the least recognized in the workplace today.

Over the last 20 years at ghSMART, we have been able to empirically observe where executives excel and where they get in their own way. We have conducted five-hour interviews with more than 15,000 leaders across every major industry, producing more than 9 million data points.

So, what is the No. 1 most common mistake that holds leaders back?

The complete inability to remove underperformers.

And why do we all struggle with this? Here are the top five reasons that we see:

1. You are an eternal optimist. You somehow believe that you will fix poor Mark in Finance or Emma in Marketing. Or, even better, perhaps they will magically fix themselves.

2. You don't want to rock the boat. You believe in accepting the cards that you are dealt. You have been taught to make do. As kids learn at daycare today, "You get what you get and you don't get upset."

3. You dislike conflict. Difficult conversations are difficult. So it is easier to suffer through it even if your whole team can now get less done.

4. You will look bad. You may have hired or promoted them into the role. You don't want to just pass the buck.

5. You excel at procrastinating. Why do today what can safely be put off for another day? Besides, who knows? He or she might resign, and that would make it easier for everyone.

You may suffer from just one, or more likely a combination, of these reasons. And yet our research found that executives who excelled at removing underperformers from their teams are more than twice as likely to have had a successful career than all other senior leaders.

Yes, that's right: twice as likely. The best leaders we meet tell us that it makes all the difference. Panos Anastassiadis is one who does it very well. He was the CEO of Cyveilance, which grew over 1500% in five years. His secret? "I have simply been constantly averaging up who is on the team." Yet how do you do that and still do right by the individual in question?

You can set them clear goals and craft the role to play to their strengths. But when it clearly isn't working, it's time to take action. Run a fair, objective talent management process, tell them that their performance isn't where it needs to be and give them 30, 60 or 90 days to turn their situation around.

If that doesn't work, it's time to have that tough conversation that deep down you know you should have had six, 12 or maybe 24 months ago.

Once done, yet only then, can you hire that A player you really need.

Geoff is Chairman & Founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the *New York Times* bestselling book *Who: The A Method for Hiring* and the author of the #1 *Wall Street Journal* bestseller *Leadocracy: Hiring More Great Leaders (Like You) into Government*. Geoff co-created the Topgrading brand of talent management. Geoff is the Founder of two 501c3 not-for-profit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring and The Leaders Initiative™ seeks to deploy soci-ety's greatest leaders into government. Geoff earned a B.A. in Economics with Honors from Northwestern University, an M.A., and a Ph.D. in Psychology from Claremont Graduate University.

The Top 3 IT Oversights Many Businesses Make

Want to avoid the most common and expensive computer problems most business owners experience? Then read on! We've compiled a list of three things you should be doing to save yourself a lot of time and money by avoiding a big, ugly computer disaster.

Have An Automated Offsite Backup System in Place

We're broken records about this but cannot stress the importance of this enough. Having an offsite copy of your data will be the equivalent of wearing a seatbelt in a major accident. You don't think much about it until you need it, and then you will thank your lucky starts you had it in place.

Centralize Your Data On Your Server

At one time, servers only made sense for large organizations because of their high cost and complexity. But today, there are very affordable and easy-to-implement server systems designed for any size small business. Depending on your business needs, your server can be in your office or hosted in the cloud. A server will not only speed up your network, but it will also make backups simpler, allow secure remote access to allow you and your employees to work from home or on the road, and make it much easier to share documents, databases and printers.

Keep Your Anti-Virus Software Up to Date

Also, perform weekly spyware scans. Everyone understands the importance of anti-virus software, but many do not perform weekly spyware sweeps. Spyware can cause a host of problems that include slowing down your systems, pop-up ads, and even identify theft.