ISSUE 6-4

BITS & BYTES

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

IN THIS ISSUE

APRIL
2015

"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

Windows Server 2003 Set To Expire July 14th!!!

If your organization is currently running either Microsoft Windows Server 2003 or Exchange 2003 on any servers in your office, you need to know about a dangerous security threat to your organization that must be addressed very soon.

Windows Server 2003 and Exchange 2003 Replacements MUST Be Made By July 14, 2015

Microsoft has officially announced that it will retire all support on the Server 2003 operating system on July 14, 2015. That means any business with this operating system still running will be completely exposed to serious hacker attacks aimed at taking control of your network, stealing data, crashing your system and inflicting a host of other business-crippling problems you do NOT want to have to deal with.

This is such a serious threat that the US Department Of Homeland Security has issued an official warning to all companies still running this operating system because firewalls and antivirus software will NOT be sufficient to completely protect your business from malicious attacks or data exfiltration. Running Server 2003 will also put many organizations out of compliance.

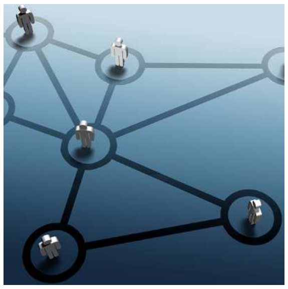
If you don't want cybercriminals running rampant in your company's computer network, you MUST upgrade any equipment running this software.

FREE Windows Server 2003 Migration Plan Shows You The Easiest, Budget-Friendly Way To Upgrade Your Server

During April and May, we are offering a FREE customized Windows Server 2003 migration plan to all businesses still running this operating system on any computers in their office. At no cost, we'll conduct a full analysis of your network to help you determine what specific servers will be affected by this announcement. Additionally, we will provide a detailed analysis of all upgrade options available to you, along with the pros and cons of each option. While there, we will also assess other security, backup and efficiency factors that could be costing you in productivity and hard dollars. We will then put together a customized Server 2003 Migration Plan specifically for your office.

To schedule your FREE on-site assessment today, e-mail Joe Stoll at
JStoll@TechnicalActionGroup.com
or call
416-489-6312 x 204.

It Might Be Time To Reevaluate Your VPN



Accessibility and mobility are important parts of a business's data infrastructure. To this end, some businesses take advantage of a Virtual Private Network (VPN), which has the power to extend a personal network over a public network like the Internet. However, with new services like cloud computing gaining traction, is it time for businesses to switch up their VPN policies to stay relevant in their industry?

VPNs are a common means to extend the reach of your business's network. They are often used by remote workers to access corporate data locally through their Internet-connected devices while on the go. This, in turn, allows for increased productivity and availability of mission-critical information. However, with the advent of cloud computing and the immense amount of new Internet-connected devices entering the market (thanks to the Internet of Things), your VPN solution might be in need of a good evaluation. To find out how your current solution holds up, it's important to see how the cloud and other new technologies are going to affect it in the years to come.

Considering the Cloud

According to Processor magazine, the cloud is changing the way that company's look at VPNs and mobile computing in general. VPNs are a technology that's been around for a while, and it hasn't changed much since its inception; unlike the cloud, which is growing more popular and dynamic by the day. For instance, many VPN users might only be using it to manage their own on-site network, and their particular solution isn't designed to cope with the advances in cloud technology. When considering that your business's data will be directly available for anyone able to connect to your network, it's important to take into account the different ways a user will access that data. This includes mobile access points, wired connections, and even through the cloud.

Security and Identity Authentication

This, naturally, leads businesses to a solution which should be designed with security in mind. The purpose of the VPN is to provide users with a secure avenue of access for confidential corporate files, even if the WiFi hotspot is sketchy at best (think free hotel WiFi). Therefore, you need to ensure security if you're hoping to reap the benefits of a VPN successfully.

According to James McCloskey at Info-Tech Research Group, "If a person is [connecting via VPN] from an unmanaged, non-corporate device, you do really want to make sure they're not going to be in a position to intentionally or otherwise access resources they don't need and store them on their local machine." This is a very real risk that is associated with VPNs and must be addressed if you want to continue taking advantage of one.

Technical Action Group's VPN solution is capable of maximizing the security of your business's network while taking advantage of a flexible, easy-to-use solution. Additionally, with our other managed IT services, we can augment your VPN with cloud management, security services, or a mobile device management solution.

If you're not sure how to approach a reevaluation of your network security and performance, we'd be more than happy to lend you our expertise on the subject. Give Joe Stoll a call at 416-489-6312 x 204 or JStoll@TechnicalActionGroup.com today for a free analysis of your network security and efficiency. Together, we can help your business achieve optimal productivity with your technology and push your bottom line to greater heights.

Shiny Gadget of the Month

The WayTools TextBlade

When we are surrounded by touch-screen mobile devices, sometimes we can get a little nostalgic for a good old-fashioned keyboard. Sure, there are a number of apps that make typing on a touch-screen easier, but tactile feedback is non-existent. Or we want to type something more substantial than a text message or quick email, and we don't want to go through the chore of typing it all out on a small screen. And then it's often hard to find a wireless keyboard that is both practical and truly portable.

The WayTools TextBlade aims to solve these problems. The TextBlade offers a fully-featured and responsive solution—while maximizing portability. Through a Bluetooth connection, you can sync it up to your favorite smartphone or tablet. The lithium polymer battery lasts upwards of a month with average use, and it's quickly recharged via USB. Small but powerful magnets keep it held in place when you're using it and when it's tucked away in your pocket.

It's priced at $99 USD and you can find it online at www.waytools.com

Imagine Losing Your Star Employee…

How Key Person Life Insurance Can Protect The Future Of Your Business

As a business owner, you may employ at least one individual who is essential to your company's success. This person may be a partner, or have a unique expertise that is unmatched throughout the rest of the company. If this person's exit from the company is planned, such as retirement or voluntary termination, then you can prepare for the loss and take the necessary precautions to minimize the impact. However, if the departure is unplanned due to an unexpected death, disabling accident or a sudden quitting, then the company is exposed to financial risks.

If you employ individuals who are vital to your company's success, especially if your business is small, consider key-person life insurance. This insurance solution can protect your organization's solvency in the event that you lose the key person without warning, and also the investments made by lenders and investors to your company.

Advantages of Key-Person Life Insurance

- Can be easily implemented
- Life insurance benefits are paid to the company tax-free
- Customers, creditors, lenders and stockholders have the assurance that the business has a continuation plan and coverage in place
- There is flexibility in what the funds can be used for

How Does Key-Person Life Insurance Protect Your Company?

- You purchase life insurance on the key individual(s).
- You are the beneficiary of the life insurance policy, and apply for and own the policy. If the key employee dies prematurely, the policy pays out to you.
- Tax-free dollars from the policy can be put towards finding, hiring and training a replacement employee, compensation for lost business during the transition and/or financing timely business transactions.
- Policy can be transferred to a departing key employee as a retirement benefit or to a different key individual, upon the retirement of the original key employee.
- Can be used to buy out the key employee's shares or interest in the company.
- Premiums are based on several factors, including the key employee's age, physical conditions and health history. The amount of coverage also affects the premium.

Considerations to Ponder…

Would losing one of your employees have one or more of the following effects?

- Jeopardize your financial security?
- Create a loss of a specialized skill?
- Disrupt everyday business operations?
- Create customer concern due to a loss of expertise?

Mumby Insurance Brokers, Inc., Your Coverage Expert

What's your business insurance done for you lately? Mumby Insurance Brokers provides more expertise, professional and objective advice, specialized attention, insurance options, and regular communication to ensure that you and your business are well-protected. FOR ANY QUESTIONS OR MORE INFORMATION, CONTACT Kelly Wilson at Kelly@Mumby.com or at 800-446-5745 x 229

2 Smart Productivity Tips to Slash Stress Levels

We all know the story of the overworked employee (you're probably an overworked business owner yourself!) They put everything they have into their job, but they still don't know why they can't get everything done on time, or why their work productivity suffers. The truth of the matter is that they are pushing themselves too hard. If you want to be truly productive, you need to work smarter and more economically. Don't burn yourself out by working too hard.

Instead, do things the right way, and you'll never feel like you're working again.

Start a Routine

If you are just haphazardly completing tasks one after another, you probably won't be able to notice the difference between "completing tasks" and establishing a routine. The difference is that a routine is optimized for efficiency and maximum production, where completing tasks is likely frantic and disorganized. Wake up at a certain time every morning. Spend a set amount of time checking your email. Try to keep your routine as consistent as possible.

Create a To-Do List

On a similar note, you should outline your days, weeks, and even months ahead of time, if you can. Assign large projects to particular days, and you won't have any trouble remembering that they must be done. Having a solid schedule will also let you stay busy without overburdening one particular day to. finish a project on a tight deadline.

Does This Password Sound Familiar?

You know the difference between a good password and a bad one. Many of us do like the convenience of a simple, easy-to-remember password that requires no effort to recall and type when we connect to our WiFi network, buy from our favorite e-tailer or use for online bill pay. But many of us also appreciate an added layer of security so we **don't** use an effortless password when sensitive data is on the line.

In a recent study conducted by SplashData, they looked at a sampling of over 3 million passwords (all of which were leaked during a data breach last year). They compiled a list of the most common passwords—and the results weren't all that surprising. **123456** was the No. 1 password used last year, followed by the classic **password**.

While these passwords may have the IT and security crowds shaking their heads in dismay, it's not all bad news. These popular passwords may offer next to no practical security, but according to the study, the 25 most common passwords only represent about 2% of the overall total.

This means most people don't use these passwords—or **qwerty**, or **111111**, or **iloveyou**. The study found more variation among the most popular passwords versus the 2013 study. Is it a possible trend? Are people turning to more imaginative or secure passwords? Maybe, but only time will tell. Even if the study suggests most of us don't rely on overly simple passwords, SplashData's list serves as a reminder to use more secure passwords and to change them regularly.

Worldwide Security Threat Services Spending To Exceed $1.4B by 2018

It's true that security threats should always be top of mind for today's SMBs. In addition, another thing to think about is a consistent bombardment of unknown, targeted, and adaptive cyber threats that are wreaking havoc in the enterprise and driving the expansion of threat intelligence security services (TISS) that are specifically designed to detect advanced persistent threats (APTs), advanced malware, and previously unidentified attacks. According to new research from International Data Corporation (IDC), worldwide threat intelligence security services spending will increase from $905.5 million in 2014 to more than $1.4 billion in 2018.

The TISS market is made up of several distinct facets, including data feeds and publications, consulting security services, and managed security services (MSS). IDC has expanded its definition of the intelligence security services market to include what it calls iterative intelligence. This iterative process learns from past experiences and mistakes, and incorporates this new knowledge at a more rapid pace, which often results in better long-term solutions. Additional findings from IDC's forecast include the following:

· TISS consulting services make up roughly 22% of the 2013 TISS revenue.
· Iterative intelligence must be available to small and medium-sized businesses as they see increased attacks like wire fraud and intellectual property theft.
· Both professional and managed security services will continue to experience strong growth in the threat intelligence arena.
· TISS offers customers deeper insights into global threat environments than they could achieve themselves.
· Security services firms are creating alliances with universities and accreditation programs to find and develop security personnel.

3 (More) Smart Productivity Tips to Slash Stress Levels

Prioritize Tasks

Going along with the first few tips, look at what needs to be done and what is most important. You're busy, and you know what tasks should be completed and prioritized. Hand off lesser work to others who are capable. This also promotes more teamwork and collaboration between departments, which can be beneficial in the long run.

Set a Deadline, and Stick to It

This is an absolute necessity for large projects, and even smaller projects. If you don't tell yourself that you need to get something done, you won't get it done. It'll just sit there and collect dust until you finally set a deadline for it, and then you'll scramble to get it done on time with subpar results.

Instead, work on it a little bit every day with an overall deadline in mind. Set this deadline a few days before it is due to ensure that you come up with the best quality work that you can.

Keep Your Work at Work

Central to any successful smart working scheme is to separate your work life from your home life. While at the workplace, avoid distractions such as social media, text messaging, phone calls, and Internet browsing. You'll find yourself accomplishing more in the workplace and relaxing more at home, away from the stress that the workplace causes.