BUSINESS CONSULTANTS WITH A TECHNOLOGY FOCUS ISSUE 104 October 2017

TECHSAGE TECH TALK

"Insider Tips To Make Your Business Run Faster, Easier, and More Profitably"

Happy Halloween

October 2017

This Monthly Publication provided courtesy of John Hill, President of TechSage Solutions.

We are Business Consultants with a Technology Focus and have Leveraged Technology to Propel Our Clients Toward Competitive Success in the San Antonio area for sixteen years. Our goal is to Simplify the use of Information Technology for our Clients so that they can focus on managing and growing their businesses.

You're Better Off Giving Your Employees A $1,000 Bonus Than Being Cheap With Technology

Imagine, for a minute, that you're the CEO of a scrappy, promising new start-up. In the beginning, it was just you and two other employees working on dinky PCs out of a 12-by-12-foot office, but times are picking up and the company is heading into the uncharted waters of rapid growth.

As the business moves into the public eye — and, in turn, the hungry eyes of potential hackers — it's become obvious that you're going to need to lock down your data. At this critical stage, a cyber-attack could mean the death of everything you and your team have built.

But the budget is looking lean. Everything you've done so far has been by the skin of your teeth, so why should security be any different? You put one of your more tech-savvy employees on the case, tasking him with finding the cheapest cyber security solutions available. Sure, he may not be an expert, but he understands computers. What could go wrong?

He scours the web, perusing dozens of "Top 5 Cheap Firewall Software" articles, and, with the help of a scrappy how-to guide, installs what seems to be the best of the lot on your servers and across all your computers. The entire process takes 10 hours, and costs the company next to nothing.

Potential crisis averted, you turn your attention to other matters. We'll revisit our cyber security later, you think, once we have a little more financial wiggle room.

Across the following year, the company's success skyrockets. The phone is ringing off the hook, new business is flooding in

Continued on pg.2

Continued from pg.1

and your profit margin is exploding. You even ended up snagging a feature in *Entrepreneur* magazine. Your company is the envy of all your peers.

That is, until the day that you get hacked. One morning, an advanced strain of ransomware easily sidesteps your free antivirus and starts wreaking havoc. It slithers through your systems and locks you out of *everything*, from client data to basic Word documents, and encrypts it behind a paywall, demanding $50,000 in Bitcoin or you'll lose access to all of it — forever.

You couldn't make room in your budget for a robust cyber security solution. Well, how does that $50K ransom strike you?

This may sound like nothing more than a horror story, but in reality, this happens to business owners all over the world each and every day. An IBM security study from last December discovered that over half of businesses surveyed had paid over $10,000 in ransomware payoffs, with 20% paying over $40,000. And that's not even including the millions of dollars of damage caused by other forms of malicious software every year.

> **"The fact is, when your time, money and business are on the line, it simply doesn't pay to be cheap when choosing your cyber security technology."**

The fact is, when your time, money and business are on the line, it simply doesn't pay to be cheap when choosing your cyber security technology.

Think of it this way. Say, with your free antivirus, you're "saving" $100 a month. Lo and behold, a virus manages to punch its way through and causes chaos throughout the company server. Even if you're lucky and it isn't ransomware, by the time you've managed to expunge the stubborn virus from your business, you'll have put in countless man-hours, guaranteed to cost you more than that $100 a month. Instead of throwing those thousands of dollars down the drain, you'd be better off giving each of your employees a $1,000 bonus!

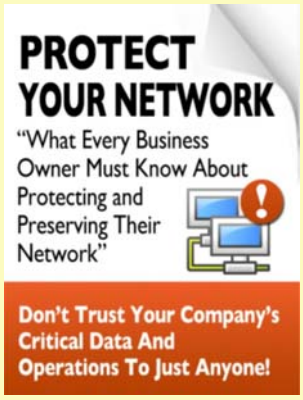
Free antivirus software, giveaway cyber-protection, or a $5 firewall seems like a great idea, until a hacker cuts through your company's defenses like a warm knife through butter. These guys *love* when they see these outdated, cheapo barriers guarding your priceless data — those are the paper-thin defenses that keep hackers in business.

You wouldn't buy a rusty, secondhand old lock for your house, so why are you installing primitive cyber security software to protect your most precious company resources?

In today's world of rampant cybercrime, it's inevitable that somebody will come knocking at your digital door. When that day comes, do you want a free piece of software that you saw on LifeHacker, or a tried-and-tested, up-to-the-minute, comprehensive security solution?

Don't be shortsighted and risk everything just to save a quick buck. Invest in your company's future, and protect yourself with the most powerful tools on the market.

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



This report will outline in plain nontechnical English common mistakes that many small-business owners make with their computer network that cost them thousands in lost sales, productivity and computer repair bills, as well as providing an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at
www.techsagesolutions.com/protect
or call our office at (210) 582-5814

Please join TechSage Solutions to explore how your business is under ATTACK and ways to protect yourself from the growing number of ATTACKS.

During This Must-Attend Seminar You'll Discover:

- **The scary risks of mobile and cloud computing – and critical policies, procedures and protections EVERY business must have in place NOW to protect themselves;** overlook even one and you're exposing yourself to security breaches, damaging and expensive litigation, employment lawsuits and having confidential company information exposed to competitors, hackers and cyber-criminals.
- The **#1 security threat to your business** that antivirus, firewalls and other security protocols are defenseless against.
- **Why firewalls and antivirus software give you a false sense of security—**and what it REALLY takes to protect your organization against new threats and today's sophisticated cybercrime rings.

Who Should Attend?

C-Level executives and managers who are concerned about: lost or stolen devices, privacy of confidential information, employment litigation introduced when employees use personal devices to access company data and State and Federal laws that carry heavy fines for lost or stolen data. This is of particular importance for those organizations that handle ANY sensitive data such as credit card and financial information, medical records (or serve clients who have medical records) or who simply want to avoid having their bank account wiped out due to a cyber-attack.

Event Details

When: November 9, 2017
Session Time: 11:30 am—1:00 pm
Where: San Antonio Technology Center Web Room
3463 Magic Drive
San Antonio, Texas 78229

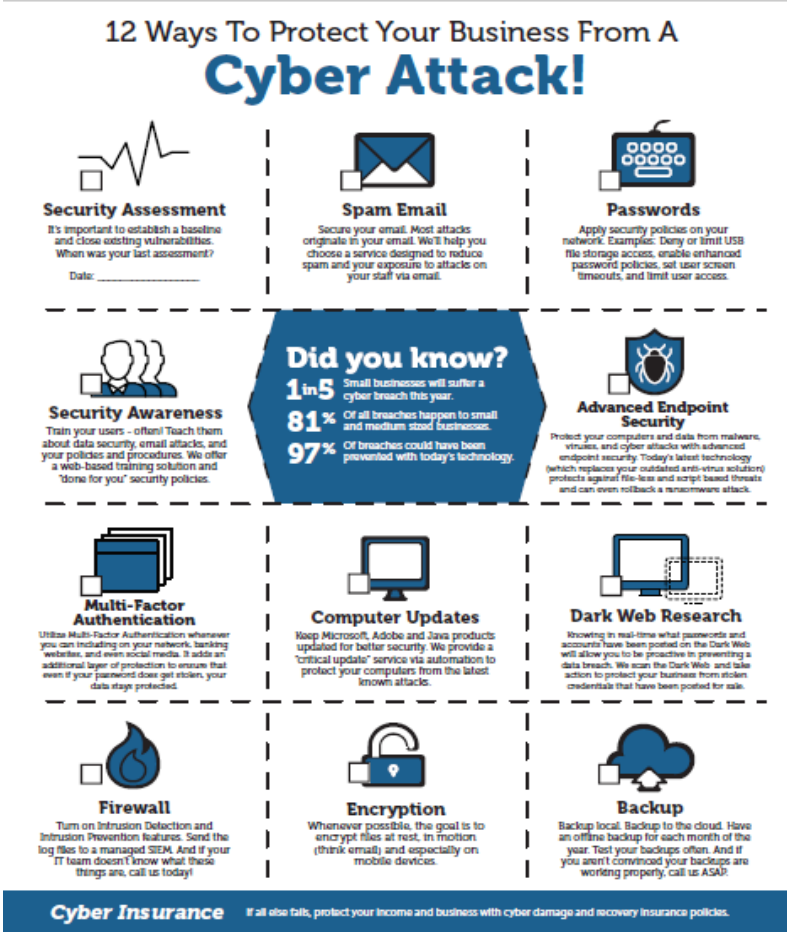
Event Catered by: Blanco BBQ

Register Event Link: www.techsagesolutions.com/cybersec2017/

and Co-Host

Thank you to our sponsors:

Is Your Business Protected?



Referral Contest!!

Refer a friend to TechSage Solutions between July 1, 2017 - October 31, 2017 for a YETI Roadie 20 Cooler. A qualified lead places your name in the drawing.

How the Contest Works:

1) Call or email us with your referral information.
2) We will call to schedule an appointment.
3) We will pay you or donate $25 to your favorite charity for anyone that you refer to us, who we get an appointment with.
4) When your referral becomes a client (and spends $1,000 or more), we will pay you $75 more or donate $75 more to your favorite charity. Plus, we will give your referral $100 off the purchase.
5) What makes a good referral for TechSage Solutions? A business owner who has 10 or more PC's and needs help with their network, data backups, email server or is just interested in having a second opinion on how they are doing things now. We provide service to the San Antonio area and surrounding cities.

Send an email to info@techsagesolutions.com or call (210) 582-5814

SHINY NEW GADGET OF THE MONTH: Picture Keeper Connect, The Best Way To Back Up Photos On The Go

Nothing feels worse than having to delete an old favorite to make room for some new photos. The Picture Keeper Connect solves both of these issues, providing easy-to-use backup for your phone or tablet.

The Picture Keeper Connect, which looks a lot like a conventional flash drive, is designed specifically to back up photos, videos and contact information with just a couple of button presses. It plugs into your phone and gets to work. Even better, it can do all of this without the need for WiFi or network connection. It keeps your photos in their designated album, meaning you won't end up with a cluttered mass of photos when you transfer them to a new device.

Simple, functional, and portable, the Picture Keeper Connect is a must for any avid smartphone photographer.

Quick And Dirty Digital Strategies

Everyone knows that a digital presence is vital for contemporary business success. According to TechCrunch, over 79% of Americans shop online these days, a massive market that you're missing if your website isn't optimized or fails to offer online payment of shopping options. Even if your business doesn't sell products that lend themselves easily to an online storefront, you can bundle the knowledge you have on offer into an e-book or pamphlet. This will allow prospects to "shop around" with your company without actually having to make a purchase, establishing you as an expert in the field and capturing leads.

What is Spooky, When You Find Out Your Passwords Are Being Sold On The Dark Web

TechSage Solutions has a new offering. With the intense increase of cyber crime, we are continuous looking for products to help your company's security. The basic security of anti-virus and a firewall is not enough to protect a business any longer.

TechSage Solutions now has the ability to detect your compromised credentials in real-time on the Dark Web. Using a proprietary technology, Dark Web ID vigilantly searches the most secretive corners of the Internet to find compromised credentials associated with your company, contractors and other personnel, and notifies you immediately when these critical assets are compromised, before they are used for identify theft, data breaches or other crimes.

Do you have any concerns that your company may have been exposed on the Dark Web. Call us today at 210-582-5814 to find out!

Equifax Hack, important steps you can take now to help protect your information

There is a lot of criminal activity in the cyber world with the goal to steal your information. The recent Equifax hack will affect many.

√ If you have not already done so, you should place a freeze on your credit with all three credit bureaus, Transunion, Experian and Equifax.

√ Consider a credit monitoring solution.

√ Do not give out any personal information to anyone unless you know you are talking to a legitimate organization. It is best to look up the phone number and contact your bank or credit card company.

√ Update your passwords.

√ Sign up for alerting on all bank accounts and credit cards. Contact your financial institution immediately for any suspicious activity.

A Diverse Team Is More Productive

Everyone knows the saying, "If you build it, they will come," from the 1989 film *Field Of Dreams*. Well, the same rule applies to the type of work environment you create, and, as a result, how diverse your team becomes.

Diversity may not happen overnight, but you can be sure that a diverse team means a broader range of perspectives brought to the problem-solving table. When employees feel accepted and comfortable in their workplace, you can expect them to take more chances on out-of-the-box thinking and creativity, not to mention increased productivity.

But you can't expect your employees to feel safe expressing their identities, and thus their ideas, if you don't first create an inclusive environment for them. But how do you create a space in which your team feels safe drawing from their unique perspectives?

One way to make your employees feel more visible and heard is through **diversity networks**, groups that come together based on shared identities, like single moms, veterans, LGBTQ individuals, Asian-Americans, Latin-Americans or disabled individuals. These networks help individuals support and learn from one another, share resources and discuss the challenges and stereotypes facing this facet of their identity and how to address them. If you're worried that this could divide the office more than unite it, don't be. These networks empower individuals to share their experiences with the broader team, allowing everyone to learn from each other.

You also need to make sure you **allow opportunities for team members to express themselves**. The quickest way to make an employee feel uncomfortable and unaccepted is to have their co-workers interrupt or speak over them. Provide moments for individuals to talk about the projects they are working on, their goals and their struggles.

Diversity training can be helpful in the office. The fact is, everyone has a bias, and it's usually subconscious. Diversity workshops can be a great way to unpack our biases and privilege. Being able to listen and empathize is a vital skill in any business setting, and will improve not only communication between your employees, but their customer service skills as well. A diversity workshop should not be a lecture, but rather an opportunity for honest conversation and learning.

Institute an open-door policy so that your employees feel safe coming to you and their other bosses about issues of discrimination, sexism, racism, homophobia and more. First and foremost, listen. Don't invalidate their experiences by immediately questioning them or taking a side in the conflict. This, plus literally keeping your door open as often as possible, will instill a feeling of trust in your office.

Show that diversity is important to you by hiring employees who come from a variety of backgrounds. Your work team should ideally represent the full diversity of your customer base, enabling them to relate and appeal to your clients on a personal level. Representation also works as a strong motivator. When individuals can see themselves in their role models — bosses, podcast guests, interviewees, etc. — they'll be more likely to imagine higher goals for themselves.

MIKE MICHALOWICZ (pronounced mi-KAL- o-wits) started his first business at the age of 24, moving his young family to the only safe place he could afford-a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group, a consulting firm that ignites explosive growth in companies that have plateaued; a former small business columnist for The Wall Street Journal; MSNBC's business makeover expert; a keynote speaker on entrepreneurship; and the author of the cult classic book The Toilet Paper Entrepreneur. His newest book, The Pumpkin Plan, has already been called "the next E-Myth!" For more information, visit www.mikemichalowicz.com/

IT Security Tip #33: Physical Security matters!

In a recent incident reported in US news, an office secretary unknowingly gave some of her law firm's most private data to a gentleman who had bought a Comcast Cable polo shirt off eBay. He dressed in khakis with a tool belt, and told the secretary he was there to audit their cable modem specifications and take pictures of the install for quality assurance. She had no reason to suspect he was part of a now-extinct hacker ring who would gain access to a business's private network by going inside the office and noting the configuration details and passwords for their firewalls and cable modems. In some cases, they actually built a secure VPN private backdoor they later used to steal data. If someone dressed up in a utility-provider uniform, would you let them in?

Ask for identification and who they have spoken with about the service they are performing, and be gracefully suspicious, as they say in the South. Keep any company policies about how visitors are allowed in the building, if such policies exist. If those kinds of policies don't exist, work to define them. We can help, if needed – but this is a real problem your office needs to address.

Sign up for our weekly Security Tips :

www.techsagesolutions.com/cybersecuritytips/