

TECHSAGE TECH TALK

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

Happy
Halloween



October 2016



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.



Could One Tiny Leak Wipe Out Your Entire Company?

Things were going great at Michael Daugherty's up-and-coming \$4 million medical-testing company.

He was a happy man. He ran a good business in a nice place. His Atlanta-based LabMD had about 30 employees and tested blood, urine and tissue samples for urologists. Life was good for this middle-aged businessman from Detroit.

Then, one Tuesday afternoon in May 2008, the phone call came that changed his life. His general manager came in to tell Daugherty about a call he'd just fielded from a man claiming to have nabbed a file full of LabMD patient documents. For a medical business that had to comply with strict federal rules on privacy, this was bad. Very bad.

It turned out that LabMD's billing manager had been using LimeWire file-sharing software to download music. In the process, she'd unwittingly left her documents folder containing the medical records exposed to a public network. A

hacker easily found and downloaded LabMD's patient records. And now the fate of Michael's life – and his business – were drastically altered.

What followed was a nightmarish downward spiral for LabMD. Not one to go down without a fight, Michael found himself mired in an escalating number of multiple lawsuits and legal battles with the Federal Trade Commission and other regulators investigating the leak.

Finally, in January 2014, exhausted and out of funds, his business cratering under constant pressure, he gave up the fight and shuttered his company.

One tiny leak that could have easily been prevented took his entire company down. Could this happen to you and your business? Let's take a look at four fatal errors you MUST avoid, to make sure it never does:

Have you developed a false sense of security?

continued on pg2

Leveraging Technology to Propel Our Clients Toward Competitive Success

Please, please, please do NOT think you are immune to a cyber-attack simply because you are not a big company. The fact is, whether you have 12 clients, or 12,000 clients, your data has value to hackers.

A simple client profile with name, address and phone number sells for as little as \$1 on the black market. Yet add a few details, like credit card and Social Security numbers, and the price can skyrocket – \$300 per record is not uncommon. Being small doesn't mean you are immune.

Are you skimping on security to save money? Sure, of course you have a tight budget... So you cut a deal with your marketing manager, who wants to work from home at times. He links into the company network with a VPN. If configured properly, your VPN creates a secure and encrypted tunnel into your net-

work. So his device now links his home network into the company network. The problem is, his home cable modem may be vulnerable to attack, an all-too-common issue with consumer devices. Now you have an open tunnel for malware and viruses to attack your network.

"You MUST remove those accounts without delay."

Could lack of an off-boarding process put your company at risk? It's crucial to keep a record of user accounts for each employee with security privileges. When an employee leaves, you MUST remove those accounts without delay. An internal attack by a disgruntled worker could do serious harm to your business. Be sure to close this loop.

Have you been lax about implementing security policies for desktop computers, mobile devices and the Internet? The

greatest threat to your company's data originates not in technology, but in human behavior. It starts before you boot up a single device. In an era of BYOD (bring your own device), for instance, lax behavior by anyone connecting to your network weakens its security. Your team love their smartphones, and with good reason. So it's tough sticking with strict rules about BYOD. But without absolute adherence to a clear policy, you might as well sell your company's secrets on eBay.

Don't let a tiny leak sink your ship – here's what to do next...

Let us run our complete Network Security Audit for you. We'll send our top data security specialist to your location and give you a complete top-to-bottom security analysis with action plan. This is normally a \$297 service. It's yours FREE when you call now through the end of October.

Don't wait until disaster strikes. Call 210-582-5814 to schedule your FREE Network Security Audit TODAY.

Free Report Download: If You Are Considering Cloud Computing For Your Company, DON'T, Until You Read This...

INTRO TO CLOUD COMPUTING

"5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud"



Discover What Most IT Consultants Don't Know Or Won't Tell You About Moving Your Company's Network To The Cloud

If you are considering cloud computing or Office 365 to save money or simplify IT, it is extremely important read this special report, **"5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud."**

This report discusses in simple, non-technical terms the pros and cons of cloud computing, data security, how to choose a cloud provider, as well as three little-known facts that most IT consultants don't know or won't tell you about cloud computing that could end up causing you MORE problems and costing you more money than you anticipated. **Even if you aren't ready to move to the cloud yet**, this report will give you the right information and questions to ask when the time comes.

Get Your Free Copy www.techsagesolutions.com/cloudreport/

Cloud Solutions • Co-Location • Disaster Recovery Planning & Data Protection

www.TechSageSolutions.com

Announcing Upcoming Cyber Security Seminar on October 13, 2016

Please join TechSage Solutions and Co-Host The South San Antonio Chamber of Commerce for this exciting and scary event to find out how to protect your business from ATTACK!



Event Details:

When: Thursday, October 13, 2016

Session Time: 11:30 AM—1:00 PM
Lunch will be provided

Where:

San Antonio Technology Center
Web Room
3463 Magic Drive
San Antonio, TX 78229

Register:

<http://www.techsagesolutions.com/>

During This 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 anti-virus, firewalls and other security protocols are defenseless to.
- **A SHOCKING truth about bank fraud** that most businesses don't know about that could (literally) wipe out your bank account.
- **Why firewalls and anti-virus 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.

Register by going to this link <http://www.techsagesolutions.com/cybersec2016/>



San Antonio Ransomware Road Show

I recently had the opportunity to attend a "Ransomware Road Show" presented by the FBI and US Secret Service and it was packed with great information presented by two very knowledgeable agents, one from the FBI and one from the Secret Service.

One key thing they briefed is that the FBI and Secret Service are working together to provide up to date intelligence to private business about ransomware.

Cyber threats are evolving rapidly with new variants appearing every day. Each new variant requires a corresponding variation in the way antivirus or antimalware protection acts. According to Special Agent Matthew Perry, the agent in charge of the San Antonio Cyber Response team, in January through May of this year over \$9.39 Million dollars were lost by companies due to cybercrime. In 2015 roughly \$24.12 million was lost. The average ransom demand by attackers this year is \$679 per attack for consumers and small businesses. Ransom payments are normally required using Bitcoin, a virtual currency that is almost impossible to track.



5 Stages of Ransomware Attacks

Installation – The victim opens a malicious email or clicks a malicious link

Contact – The malware contacts its command and control server to get instructions

Encryption – The malware encrypts the victim's files

Extortion – Popup message on victim's computer to tell them their files are encrypted and providing instructions on how to regain access.

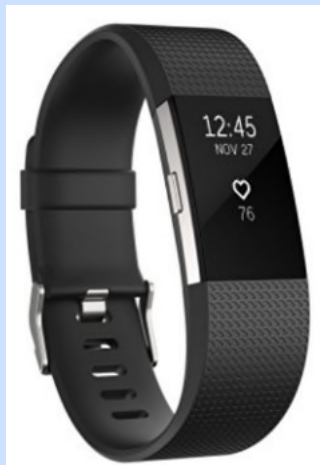
Recovery – Victim pays the ransom and receives key to recover files (most of the time)

Companies must take a multilayered approach to help protect themselves. Below are some of the suggestions to protect your business from ransomware attacks:

- Subscribing to an internet filtering service
- Subscribe to a spam filtering service
- Installing a commercial grade firewall at the perimeter of your network
- Insuring that the software firewalls built into the operating systems of your desktops
- Laptops, and servers are turned on, install centrally managed and updated antivirus and antimalware on your desktops,
- Laptops, servers and mobile devices and insure that operating system
- Software vendor patches, updates and fixes are installed and current.

Nothing can guarantee that you will never suffer from a ransomware attack, but the actions listed above can dramatically reduce the likelihood of it happening. It's also vital to educate your employees on the threats and how to avoid them.

Referral Contest!!



Refer a friend to TechSage Solutions between September 1, 2016 - December 31, 2016 for a chance to win a Fitbit Charge 2 Heart Rate. 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 ehill@techSagesolutions.com or call (210) 582-5814.



Hololens: Your New Reality?

A game designer sees a moving 3-D image of a living, breathing, mace-wielding ogre – on her desk. She flicks a finger and he turns from side to side, giving her a full view of his outfit and weapons belt.

An architect looks up at the ceiling in a building he's just designed. He waves his hand and reshapes it, allowing more light through. All virtually.

A space scientist designing a Mars rover strolls through the landscape, noting from all sides the position, shape and size of rocks his vehicle must navigate.

Now it's your turn. Put on the new HoloLens by Microsoft, and what do you see? How could you use this cool new augmented reality (AR) tool in your business?

At \$3,000 for the developer's version, it may not be an impulse buy. But new AR tools like this will soon be part of your computing world.

Dealing With The Dark Side Of Social Media

Social media has become a true amplifier, permeating every nook and cranny of the web, giving a megaphone to those who might have previously found themselves voiceless.

While I generally believe that the proliferation of the social web is a good thing, it does have a dark side that is difficult, if not impossible, to ignore.

I was reminded of this recently when an unscrupulous competitor accused me and my friend Larry Winget of an ugly racial slur. While it was totally fabricated, this person willfully resorted to defamation of character to defend his indefensible behavior.

It's easy to get mad, get on your computer and allow emotions to run amok. And that can come back to bite you. Yet there are times you shouldn't acquiesce to digital bullies. You need to take a stand.

Here are a few tips on how to keep your social media actions in check, and how to react to others who just can't seem to control theirs:

How do I think through my social media actions in a heated moment?

If you wouldn't say it to your grandmother, don't write it on Twitter. It feels good to blast an opponent, but such outbursts can easily be used against you.

Remember that everything you say or do on the web is archived. Consider everything you write on the Internet to be permanent. Trolls may delete their comments, but they still leave a trail.

Still debating saying it? Sleep on it. If you really feel the need to say something that might be taken the wrong way, consider sitting on it overnight. Waiting until the next day will rarely hurt your point, and it may save huge amounts of embarrassment.

If you do say it...make sure you feel you could defend it in a court of law. Falsely accusing someone of something is a big deal, and the repercussions could amplify beyond your original intentions.

How do I react when I am targeted on social media?

Grab screenshots. If someone truly is going after you, the first move is to gather evidence. Make sure you have copies. Odds are that they will quickly realize what they have done and will try to erase their trail, so the best thing you can do is make sure you have a copy on hand.

Report them. Twitter, LinkedIn, Facebook and most other platforms have guards against those who harass others. Don't hesitate to put in a report – that's why those guards are there!

Remember that the truth is your best defense. As someone who has been egregiously accused of something I did not do, I took solace in the fact that I was innocent, and as such the accusation cruelly asserted could never be proven.

We live in a world where unscrupulous people have migrated to online communities and live among the rest of us. I hope you never have to use the above actions, but when you do, I hope they serve you well.



Mark Sanborn, CSP, CPAE, is president of Sanborn & Associates, Inc., an idea studio dedicated to developing leaders in business and in life. Mark is an international best-selling author and noted authority on leadership, team-building, customer service and change. Mark is the author of 8 books, including the best seller *The Fred Factor: How Passion in Your Work and Life Can Turn the Ordinary into the Extraordinary*, which has sold more than 1.6 million copies internationally. Learn more about Mark at www.marksanborn.com.

Savvy users are capitalizing on the LinkedIn-Microsoft merger.

Here are three ways you too can profit: 1) Your profile photo now appears on both platforms. Run it by photofeeler.com to make sure it's up to snuff. 2) When it comes to updates, forget text – video rules. Check your newsfeed and you'll see how LinkedIn puts video on top and is burying articles. No wonder members have seen a 60% to 90% drop in readership. To get attention, go video. 3) Keep an eye on LinkedIn's social advertising. With access to user data from both platforms, your ads could now enjoy a wider audience of both LinkedIn and Microsoft users. This merger opens new doors for users. Now's the time to capitalize on it.

-Entrepreneur

Want to know the secret to beating ransomware?

If there's one pop-up you NEVER

want to see on your computer screen, it's this: "Your files have been encrypted. You have 72 hours to submit payment or they will be deleted forever." Once ransomware hits, it's too late. Game over. The best way to beat ransomware is prevention. Make sure it never happens in the first place. And if somehow it happens anyway, make sure you have up-to-date backups ready to go. The first step to prevention is to invest in serious cybersecurity. Start with antivirus software with active monitoring. Then, layer in anti-malware and anti-ransomware programs. Finally, store current backups in the cloud and/or on a separate unplugged hard drive.

-blog.malwarebytes.com

A wafer-thin laptop so light you'll forget it's in your briefcase...

Want an ultrasleek machine with enough battery life to keep you going long hours without plugging in? A new breed of "ultraportables"

offers that and more. The lightning-quick storage on these units lets you resume work in seconds, even after they've been idle or asleep for days. The "best in breed" will cost you a pretty penny. But if you're willing to spend a little, you can get premium features. Touch screens, full HDMI ports and eight hours or more of battery life are not uncommon. At the top end, you can expect a high-resolution 4K screen (3840 x 2160). Be extra-nice and Santa might even slip one in your stocking!

-PCmag.com

Considering Facebook Live Video for your business?

Using Facebook Live is brain-dead simple. If you haven't already, install the Facebook app on your smartphone. Open it up, tap the red "Go Live" icon and you're on. It tells you how many are watching, plus their names and comments. When you're done, it saves to your Timeline. And, unlike Snapchat or Periscope, it doesn't disappear after just 24 hours. You can share, embed, Tweet – or delete – to your heart's content. And you can filter who sees it. As for content? Interview key employees, big shots in your niche or your customers. Share how you're making a new product. Or how your team relaxes. Why do it? Your customers love getting that little peek "behind the scenes."

-PostPlanner.com

Who Else Wants To Win \$25 Gift Card?

Last month, Iris Flores took the challenge by answering the trivia question correctly. She has a \$25 Google play card coming her way.

Here is this month's trivia question. The winner will receive a \$25 Saltgrass gift-card.



Japanese computer-gaming company Nintendo was founded

Email Us Now With Your Answer!

ehill@techsagesolutions.com

With Subject: October Trivia Answer