TECH SAGE TECH TALK

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

"As a business owner, 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 finally and forever!"

John Hill,
TechSage Solutions

Inside This Issue . . . e

New Security Breach Notification Laws: What You Need To Know

It's Monday morning and one of your employees notifies you that they lost their laptop at a Starbucks over the weekend, apologizing profusely. Aside from the cost and inconvenience of buying a new laptop, could you be on the hook for bigger costs, and should you notify all your clients?

Maybe, depending on where you live and what type of data you had stored on that laptop. Forty-six of the fifty states, plus Washington D.C., Guam, Puerto Rico and the Virgin Islands, have security-breach laws outlining what businesses must do if they expose any kind of client or employee personal information, and practically every single business is directly affected by these laws. (Currently, the only states without such laws are Alabama, Kentucky, New Mexico and South Dakota, but that is likely to change.)

An Emerging Trend In Business Law

Since companies are storing more and more data on their employees and clients, states are starting to aggressively enforce data breach and security laws that set out the responsibilities for businesses capturing and storing personal data. What do most states consider confidential or sensitive data? Definitely medical and financial records such as credit card numbers, credit scores and bank account numbers, but also addresses and phone numbers, social security numbers, birthdays and in some cases purchase history—information that almost every single company normally keeps on their clients.

"We Did Our Best" Is No Longer An Acceptable Answer

With millions of cyber criminals working daily to hack systems, and with employees accessing more and more confidential client data, there is no known way to absolutely, positively guarantee you won't have a data breach. However, your efforts to put in place good, solid best practices in security will go a long way to help you avoid hefty fines. The definition of "reasonable security" is constantly evolving, but here are some basic things to look at to avoid being labeled irresponsible:

- **Managing access.** Who can access the confidential information you store in your business? Is this information easily accessible by everyone in your company? What is your policy about taking data out of the office on mobile devices?

Get More Information about our Services At: www.techsagesolutions.com

- **IT security and passwords.** The more sensitive the data, the higher the level of security you need to keep on it. Are your passwords easy to crack? Is the data encrypted? Secured behind a strong firewall? If not, why?

- **Training.** One of the biggest causes for data breaches is the human element: employees who accidentally download viruses and malware that allow hackers easy access. Do you have a data security policy? A password policy? Do you have training to help employees understand how to use e-mail and the Internet responsibly?

- **Physical security.** It's becoming more common for thieves to break into offices and steal servers, laptops and other digital devices. Additionally, paper contracts and other physical documents containing sensitive information should be locked up or scanned and encrypted.

The bottom line is this: Data security is something that EVERY business is now responsible for, and not addressing this important issue has consequences that go beyond the legal aspect; it can seriously harm your reputation with clients. So be smart about this. Talk to your attorney about your legal responsibility. Then, to get more information and training on IT security, visit us online at www.techsagesolutions.com/security or call us for a FREE Security Audit at 210-582-5814.

Are You Inviting Criminals To Rob You?

The next time you think about "Checking In" with Facebook or Tweeting about your vacation, don't. Burglars are now using social media sites to target homes when people are away on vacation, business or just out at dinner.

One such web site, PleaseRobMe.com, swears they never intended to encourage burglars; however, this site pulls information from social networking sites like Twitter, Foursquare and Google Buzz to expose how much information criminals can easily learn about you online.

The Dutch developers, Barry Borsboom, Boy van Amstel and Frank Groeneveld say they like social networking, but that their goal is to shine a giant spotlight on the dangerous side effects of location sharing. Regardless of their intention, our recommendation is to keep your location private.

Why Offsite Backup?

1. Is your company's data one of your most valuable asset?
2. What would you do without your financial or customer records?
3. How long could your business survive without access to the critical customer and operational information?

The Ultimate Guide For Setting Up A "Work From Home" System For Your Staff

WORK FROM HOME GAMEPLAN
"The Ultimate Small Business Guide To Setting Up A "Work From Home" System For Your Staff"

Secrets Every Business Owner Must Know Before Installing A "Virtual Network" To Allow Employees To Work From Home, On The Road, Or From A Remote Office

If you are thinking about implementing a "work from home" program for your employees, or if you want to install a virtual network to enable your key employees to work seamlessly on the road or from a remote office, DON'T—until you read this eye-opening guide.

In this free report, you'll discover:

- What "telecommuting" is and why so many small businesses are rapidly implementing work from home programs.
- The **single most important** thing you MUST have in place before starting any work from home or remote office initiative
- How one company **saved $11 million** after implementing a work from home program, and how you can implement the same money saving strategies in your business.
- How one company slashed its turnover rate from 33% to 0% (and **increased productivity by 18%**) all by implementing a work from home program.
- How to get a FREE "Home Office Action Pack" ($97 value).
- Request your FREE

  news@techsagesolutions.com

A Simple Change That Will Generate More Leads And Customers With Facebook

If you have been using a Facebook Fan Page as a marketing tool, here's a simple strategy we've discovered that will practically guarantee you more leads. But first, a quick marketing lesson…

Marketing messages to a NEW prospect must be different than the marketing messages to an existing customer or "Fan." That's because a new prospect has no idea who you are, what you do or why they should engage with you on any level, especially honoring you with their business. For example, if you were at a tradeshow booth representing your company, you would naturally speak differently to a new prospect than someone who's done business with you before, right? Therefore, when a NEW prospect hits your Facebook page, you don't want them to see every post you've made in the past and hope that they "Like" your page. Instead, the smart thing to do is to set up a custom "Welcome" page that appears to all new "non-fans."

This custom Welcome Page should convey what you're about and make an offer to new prospects to engage with them, capture their information and get them communicating to you. This welcome page can even contain a video of you introducing yourself, your business and explaining an offer you have for new Fans. When done right, this simple addition to your Facebook page will dramatically increase the number of leads, customers and engagement from your Facebook traffic. Here's how you set it up:

Step 1) Create your landing page on a Facebook tab.
Facebook tabs aren't the easiest to create. Unless you're a talented web developer, I've found that it's easier to use a tool such as FanPage Engine 3.0 to create your tabs in Facebook (you can find this at www.fanpageengine.com). By using custom tools, you can very easily incorporate lead generation forms, videos and formatting all in one. A new tab can be created and published to your Facebook page in less than 10 minutes with this tool.

Step 2) Set your Facebook "Default Tab" for new visitors to your new, custom landing page. Facebook's definition of a "new" visitor is someone who hasn't "Liked" your page yet.

To setup your Default Tab, go to your Facebook company page and select "Edit Page," then "Manage Permissions." Next, change your "Default Landing Tab" to your new Welcome Page. Click on "Save Changes" and you're done! Remember, this page will only display for people who haven't "Liked" your company on Facebook; everyone else will go straight to your page's Wall.

Why Did The Chicken Cross The Road?
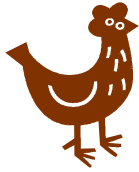
► Mark Twain: The news of its crossing has been greatly exaggerated.

► Molly Yard: It was a hen!

► Zeno of Elea: To prove it could never reach the other side.

► Wordsworth: To wander lonely as a cloud.

► The Godfather: I didn't want its mother to see it like that.

► Othello: Jealousy.

► Oscar Wilde: Why, indeed? One's social engagements whilst in town ought never expose one to such barbarous inconvenience - although, perhaps, if one must cross a road, one may do far worse than to cross it as the chicken in question.

► Kafka: Hardly the most urgent enquiry to make of a low-grade insurance clerk who woke up that morning as a hen.

► Macbeth: To have turned back were as tedious as to go o'er.

► Freud: An die andere Seite zu kommen. (Much laughter)

► Hamlet: That is not the question.

(source: popculturemadness.com)

Are You Performing *Reverse* Backups?

Here's an important question for anyone using cloud applications to host important files and data: Are you routinely downloading and backing up a copy of your files to your own servers? If not, you're taking a BIG risk of losing all that data. By now you should know to backup the data on your PCs and server offsite to the cloud; but what you might not have considered is the practice of downloading your data from critical cloud applications as a security measure against that cloud provider closing their doors, losing your data or simply cutting you off.

True Story: A business colleague hired a new web designer to update her web site. After 6 months of delays and poor service, she notified the designer that she would no longer need their services. This firm's developer then decided to delete all the web sites she had to get revenge. Apparently, the web hosting company had a "glitch" (as they called it) in their password and security system that allowed this company to gain access to her account after she deactivated their login. Fortunately, her OLD web designer had a copy of her web site, even though it was out of date. This little fiasco caused her web site to be down for a week and cost her thousands in getting the sites back up.

Point is, the more data you host in cloud applications, the more cautious you need to be in keeping a current record of those files in-house; and with more and more software companies ONLY offering a hosted or cloud version of their software, you often won't have a choice but to move your systems and data to the cloud. As a second precaution, you should review your cloud provider's policy on closing your account. In some cases, they have all the power and will shut off your access and even delete your data without warning, never to be recovered. That's why it's absolutely critical that you perform "reverse backups" of your data to your server frequently.

Who Else Wants To Win A $25 Gift Card?

Here's this month's trivia question. The first one that sends the correct answer will receive a gift card to TX Land & Cattle.

What U.S. President was elected, defeated, then re-elected?
 a) Cleveland b) Roosevelt c) Jackson d) Johnson

Send me an e-mail right now with your answer!
news@techsagesolutions.com

Happy Thanksgiving

"I DON'T TWEET, I GOBBLE."