OCTOBER TECH NEWS   **630-236-6625**   **Issue: 10**

We Hope You Find The Content Useful, Interesting and Enjoyable.

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.

In This Issue

Security Breach Laws

Reverse Back Ups

Inviting Criminals to Rob You?

QUICK LINKS

www.osgusa.com
info@osgusa.com
support@osgusa.com
www.osgusa.com/free
www.osgusa.com/freebook

SERVICES WE OFFER

· Managed IT Services
· Network Design
· LAN/WAN
· On-Site Support
· Remote Connectivity
· Microsoft Exchange Email
· Server Virtualization
· Hardware and Software Sales
· Internet Bandwidth Security
· Cloud Computing
· Virus Detection and Removal

For a complete list of services please visit:
http://www.osgusa.com/network-support.html

TRIVIA
First person to submit the correct answers by email to

"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?
- **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, call us for a FREE Security Assessment at 630-236-6625 ext 225.

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

anorton@osgusa.com will receive a $25 Starbuck gift card!

Entries are judged by date/time received and correctness. Include your name and phone number, the question number and the answer.

1) The first Jack-O-Lanterns were made out of what?

2) How many witches were burned at the Salem Witch Trials?

3) What phobia do you suffer from if you have an intense fear of Halloween?

4) According to superstition, a person born on Halloween has what particular ability?

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. For a Free Back -up Assessment call 630-236-6625 ext 225.

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.

At Your Service,

Outsource Solutions Group, Inc.
Phone: 630-236-6625
Toll Free: 1-888-236-6625
Email: info@osgusa.com
Support: support@osgusa.com

Forward email

SafeUnsubscribe

Trusted *Email* from
Constant Contact
Try it FREE today.

This email was sent to anorton@osgusa.com by anorton@osgusa.com |
Update Profile/Email Address | Instant removal with SafeUnsubscribe™ | Privacy Policy.

Outsource Solutions Group | 1730 Park Street, Suite 225 | Naperville | IL | 60563