TechTip Postcard

Insider Tips and Secrets to Get The MOST Out of Your Computer

What You Need To Know About Security Breach Notification Laws

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.

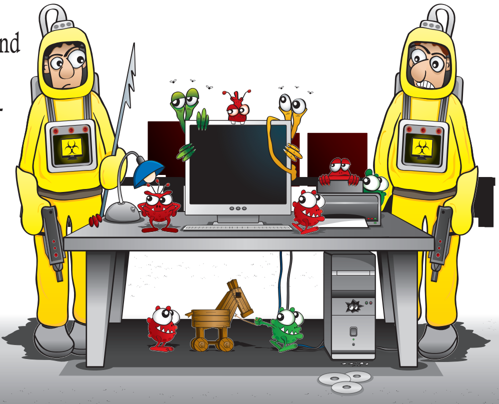
An Emerging Trend In Business Law

Since companies are storing more and more data on their employees and clients, most 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. 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.

Chris Schalleur
CEO

How Protected Is Your Business Against Security Threats? Our Free Computer Network Security Assessment (a $497 value) Will Give You The Answers

CHRISTO
IT Services
Small Business Solutions
314 Ruth Road
Harleysville, PA 19438

Claim your FREE Computer Network Security Assessment and one of our top IT security experts will:

- **Perform a vulnerability scan of your network** to determine where the weak links are.
- **Review your security and disaster recovery policies** against state and federal requirements for your industry.
- **Review your antivirus and anti-malware systems** to ensure they are working properly. This is one of the top ways that hackers can penetrate your network.
- **Review your user account settings for weak passwords and expired accounts**

Claim Your FREE Computer Network Security Assessment

Now: Go to: **www.christoit.com/cyberaudit**

Call: **215-256-7902**