

This is a printer friendly version of an article from www.fosters.com
To print this article open the file menu and choose Print.

[Back](#)

Article published Jun 14, 2009

Data security changes are in the works

If your business deals with any type of confidential data, especially that which involves personal information about your customers, you want to be aware of some important changes that are coming.

Businesses that take credit cards from their customers have had to properly secure that information for some time now. You may have heard about a regulation called PCI, which requires the safe storage of this type of data. You may also recall the very public incident when the TJX Companies, parent of the TJ Maxx retail chain, had a breach of security that exposed thousands of credit card numbers to malicious hackers.

More recently, you may have heard about a government laptop that was removed from a secure facility and brought home with classified information on it related to the military's latest jet fighter program. That data was exposed to the Internet because that laptop was not properly secured.

Incidents like these are prompting lawmakers at the state and federal level to enact sweeping legislation that will directly affect businesses of all sizes as it relates to the security of your information technology infrastructure. Right next door, in our neighboring Commonwealth of Massachusetts, a new law will go into effect at the beginning of next year that is widely considered to be the most stringent regulation of private data to date. Discussions are taking place right now, at the federal level, about these same issues. Just last week, President Obama appointed a national Cyber Security Czar to oversee this critical area of computing.

What does all this mean to your business? Simply put, it's time to get your security house in order.

The days of simple passwords, shared passwords, passwords that never expire, insecure e-mail and unencrypted file storage are coming to an end. While many feel proper IT security is an inconvenience, the fact of the matter is, you can no longer afford not to be inconvenienced at some level. Fortunately, technology continues to improve and the inconvenience of insuring proper data security is becoming far less of an issue.

There are many technologies available to address these concerns. A few that you will want to make yourself aware of sooner, rather than later, are as follows: encryption, secure communications, passphrases and two factor authentication.

Encryption technology uses an electronic key to secure the information on your hard drive, portable hard drive, USB key and even your smartphone. Without knowing the secure passphrase for the given device, the data stored there is scrambled and useless to anyone but you.

Secure communications covers a range of technologies, so let's focus on the most widely used two: E-mail and Instant Messaging. Customer information should never be discussed over public instant messaging networks like AOL Instant Messenger. If you use instant messaging for business purposes, it should be a private secure instant messaging system that runs within your company network.

I see passwords e-mailed all the time and this is a huge risk to company networks and should never be done. Encrypted e-mail, just like what I previously described, ensures the privacy of an e-mail message as it travels across the insecure Internet. Even if the message is intercepted, it is useless to the hacker. Secure e-mail encryption used to be very cumbersome to work with, but as with most things in the IT industry, the technology has evolved and has become much more efficient and user friendly. If you need to be e-mailing sensitive information, there is no reason why it should not be encrypted.

Passphrases are an evolution of passwords. How many of you use a simple password, something like your mother's maiden name or your birthday or some other easily identifiable password? Passwords like this are a main reason there are so many breaches of secure data. It's too easy for hackers to guess their way into what should be secure systems.

A passphrase is a phrase, instead of single word, and often includes numbers or other characters, to make it more secure. Two factor authentication adds another layer to passphrases, by using something called a token, that generates a customized PIN for each login request. Together, they are extremely secure.

Whatever business you are in, the point is that you need to ensure your data is secure. If you don't, you may soon face regulations that will require you to. I recommend you be proactive and ensure your business practices are truly secure.

Regardless of what legislation may come, you will be able to assure your customers that you have already instituted proper practices to ensure the security of their information and that's just smart business. Thanks for reading.

MJ Shoer is a native of Swampscott, Mass., and a 1986 graduate of the University of New Hampshire with a Bachelor of Arts degree in Political Science. Shoer worked for hardware and software technology companies from 1986 to 1995 when he became president of the first dial-up Internet Service Provider in Portsmouth. After growing and selling that business, Shoer founded Jenaly Technology Group in 1997 and serves as its president. Jenaly Technology Group provides outsourced IT services to small businesses throughout the region. Shoer is active in several IT industry groups and regularly writes about IT and small business. He lives in Portsmouth with his wife and three children.