Meet the technology challenges of compliance at your firm head-on

Kevin Shea, President
InfoSystems Integrated, Inc.

Compliance demands vis-à-vis the SEC, Gramm-Leach Bliley, and most recently emerging local regulations like Massachusetts 201 CMR 17.00, require a significant investment of resources in terms of both time and capital to meet the ever-growing regulations associated with doing business in the information age. In this article, we summarize the requirements of 201 CMR 17.00, which went into effect March 1, 2010.

Many businesses across the nation are looking closely at the law that Massachusetts implemented with the concern that similar legislation will soon be coming their way. In a nutshell, Massachusetts' new law dictates that businesses nationwide take appropriate steps to protect the privacy of Massachusetts residents' Personal Information (PI) according to their ability to do so. As such, the right solution for a small business may not be acceptable for a large business - if a more robust solution exists at a higher, yet affordable, cost for the larger business.

The new law charges businesses with the responsibility of protecting this consumer data from being lost or stolen, and may seem redundant to those familiar with the best practices from preexisting government regulations and industry standards. Companies need to know what they are up against. The threats are real. It is amazing that we have not heard more in the news about the security of private records being compromised.

The level of vigilance required to establish and maintain a secure environment at the workplace would surprise many. In truth, the only absolutely secure PC is one that is locked away out of physical reach and not connected to the Internet. The best security is established through a combination of proactive measures, and is still dependent on appropriate reactive responses to would-be hackers.

In an effort to make our checklist easier to digest, we have broken it into the four fundamental areas addressed by the law: updates, attentiveness, policy and documentation, and encryption. In the remainder of this article we take a closer look at the specific requirements of these areas.

Technology Compliance Checklist for Massachusetts 201 CMR 17.00

Updates

1. Apply operating system patches and software updates on a timely basis.
2. Reasonably current versions of Antivirus and Antispyware must be installed and updated regularly.
3. The software portion of your firewall should be kept reasonably up to date.

Attentiveness

4. Monitor your firewall and take appropriate actions when merited.
5. Perform an annual security audit.
6. Take reasonable steps to verify that third parties with access to Personal Information (PI) protect it.

Policy & Documentation

7. Create a Written Information Security Program (WISP); appoint a person at your firm to manage the program, and detail disciplinary actions associated with non-compliance by employees.
8. Create secure user authentication protocols, strict control of user IDs and passwords.
9. Any inactive employees should be removed from systems immediately.
10. Educate and train all employees about security.
11. Limit access to PI to those who specifically need it.

Encryption

12. Encrypt email that contains PI (defined as a person's name with any one or combination of the following: driver's license, social security number, financial account number, debit/credit account number, or state issued identification number).
13. Encrypt all remote access connections.
14. Encrypt backup media, notebook hard drives, portable hard drives, and all removable media that contain PI.

About the Author:
Kevin Shea is President of InfoSystems Integrated, Inc. (ISI). ISI provides a wide variety of outsourced IT solutions to investment advisors nationwide. For details, please visit www.isitc.com. You can also contact Kevin Shea via phone at 617-720-3400 x202 or e-mail kshea@isitc.com.

Updates

Downloading and applying recent security updates to your operating system and primary applications is an integral component to keeping hackers at bay. It is also a relatively low tech item that most users can take care of by themselves. Unfortunately, an occasional bad update can bring all productivity on your system to a screeching halt. This was the case with Windows XP SP3 where, in some instances, users who installed it lost their Internet connectivity.

Professional IT consultants are aware of the potential issues new updates to workstations and servers can raise. We recommend controlling the updates through Windows Server Update Services (WSUS) or opting to perform the updates manually in smaller offices. Perhaps the authors of Massachusetts' new law also recognized that all new updates should not necessarily be installed immediately. Ergo, the language indicates that systems should be reasonably up to date.

Your IT vendor should be qualified to determine exactly when updates must be applied, but if you go to the www.windowsupdate.com site and find that there are over twenty security updates to install on your PC, you should not consider your PC "reasonably" up to date.

Antivirus definitions need to be downloaded and applied regularly. Antivirus images are released by their software providers nearly everyday and sometimes more frequently. You can usually check your update by clicking on the Antivirus client program that sits on your taskbar in the lower right hand corner of your computer screen.

Keeping your firewall software reasonably up to date and security rules relevant is paramount to the security of your systems. However, only firewall patches that have been vetted by your IT staff should be installed. A bad firewall update can cause more harm than good.

Attentiveness

You will need to allocate extra resources towards maintaining and monitoring these required standards. Your firewall should be configured to log all suspicious activity, but to properly manage the security of your systems someone needs to review the logs on a regular basis and take corrective actions when required.

Though the law requires an annual audit of your security policy the reality is that it should receive much more frequent attention and amendments.

Your firm is also expected to verify that third parties with access to PI can protect it.

Policy & Documentation

Your Written Information Security Program (WISP) should spell out the policies related to keeping PI private. A person at your firm must be appointed to manage the program. Since most Massachusetts businesses have already created a WISP, you can find samples online via Google.

Secure user authentication protocol (such as limiting the number of login attempts before locking out users) are expected to be in use at your firm. In addition, passwords need to be kept private and relatively complex. If everyone at your office knows each other's passwords, you definitely need to change your policy.

When employees or contractors become inactive, their accounts must be promptly removed from your system. Educating your users is a critical aspect of securing your enterprise. Malware, for example, can be accidentally loaded by employees who do not recognize it.

Due to their size, small firms may have difficulty limiting data access to employee subgroups, but larger companies should not have as much trouble with this requirement.

Encryption

Encrypting remote access connections can be done by standardizing on Logmein, GotoMyPC, or a combination of VPN and Remote Desktop or Terminal Services.

Notebook hard drives containing PI must be encrypted. Though it is possible to buy new equipment with encrypted hard drives, you may find it easier on the wallet to purchase hardware encrypted thumb drives and enforce a policy that forbids users from saving private information on their notebook hard drives.

Likewise, any removable media such as backup tapes and/or hard drives must be encrypted. These drives are relatively inexpensive. So being a small company with limited resources will not be a valid reason for not taking care of this.

To meet the email encryption requirements for sending PI, some larger companies may elect to address the issue by encrypting all email. Smaller firms may selectively encrypt emails containing PI via Adobe Acrobat. In a perfect world, all of your clients would have a class 1 digital certificate or better and email encryption would be simplified.

If your firm performs Internet vaulting of your data, double check the encryption settings, and use 256-bit encryption or higher if possible.

This article is an interpretation of the technology issues related to the new law. To review all of the requirements, refer to the PDF link on the mass.gov web site: www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf