



The New Massachusetts Data Security Law and Your Office

Tools To Help You Comply

Presentation by Thomas N. Traina

GeekLawyer.Net



The Relevant Statutes & Regs

- ◆ The Statute

- Mass. Gen Laws c. 93H

- ◆ The Implementing Regulations

- 207 CMR 17



The Basic Requirements

- ◆ Develop a Written Information Security Plan to guide you in the event of a security breach
- ◆ Ensure all wireless transmissions and portable data storage devices encrypt sensitive personal data
- ◆ NOTE: “portable data storage device” includes your laptop!



The Technical Legal Requirements

- ◆ Create an Written Information Security Program
- ◆ Implement the plan you prepared accordingly
- ◆ Designate personnel responsible for maintaining that plan (probably ourselves)
- ◆ Monitor for compliance with the Plan and breaches of security.



How Do I Know My Plan Is Good Enough?

- ◆ “Reasonable Person” standard applies
- ◆ Takes resources of the organization into account when determining standard of care.
- ◆ In other words, Google has to do much more than you do



The Tools You'll Need

- ◆ Encryption Software
 - Encrypting Storage
 - Encrypting Wireless Networks
 - Encrypting E-Mails
- ◆ Firewall
- ◆ Antivirus Software

Good News!

You already have most of this software ready to be used!

And the rest of it is free and relatively easy to use!





What You Already Have

◆ Firewall

- Comes with most modern Operating Systems (Windows, Mac OS X, Linux)

◆ Wireless Encryption

- Your wireless router has the ability to create a “secured network” that uses encryption to protect the wireless signal from being intercepted



File Encryption - TrueCrypt

- ◆ Free to Use Software
- ◆ Effective Encryption of files on a hard drive
- ◆ Relatively simple to use



First, some technical jargon (sorry)

- ◆ A physical device (hard drive) can be divided by software into separate drives, usually called “volumes”.
- ◆ Computers don’t always know what to do with a volume you have attached to them.
- ◆ Your computer needs to do some setup to understand how files are stored on the volume.
- ◆ This process is called “mounting”.



What Does TrueCrypt Do?

- ◆ TrueCrypt creates encrypted computer files and fools the computer into thinking that they are storage devices like your hard drive.
- ◆ You can access files stored in the virtual hard drive with the password that decrypts the file used for storage.



Practical Upshot of This

- ◆ Your files are encrypted
- ◆ Your files are portable
- ◆ You can create special file containers that contain just one client's files to share with them.



E-Mail Encryption: A Big Challenge For Us

- ◆ E-Mail was not designed to be “secure”.
- ◆ All security methods that would work with e-mail require some sort of shared information.
- ◆ The most effective programs are the ones hardest to implement
- ◆ Difficulty is not in cost, but in getting others to agree to use it.



Common Solutions

- ◆ Encrypting the message contained in the e-mail (PGP)
- ◆ Redirect to an encrypted message storage site
- ◆ Saving e-mails to an encrypted storage device and deleting them from your e-mail server immediately (TrueCrypt)



PGP: The Most Secure Answer

- ◆ PGP is a protocol, not a software package*
- ◆ Users have two “keys”: private & public
- ◆ Private keys open messages closed with the corresponding public key and vice versa



How To Use PGP In Practice

- ◆ Encrypting Messages
 - A lawyer shares their public key
 - A client “closes” their message with the lawyer’s public key
 - The lawyer opens the closed message with his/her private key.
- ◆ Ensures that only those who have the private key can open the message



How to Use PGP in Practice

- ◆ “Signing” Messages
 - A lawyer “closes” their message with their private key and sends it to a client.
 - A client opens the message using the publicly available public key.
- ◆ Only a person with the private key can create a message that can be opened by the public key.
- ◆ Ensures that message actually came from the person who says they sent it.

Tools You Can Use



Firefox	Gnu Privacy Guard (GPG)	FireGPG
Web Browser	PGP Encryption Software	“middleware” between GPG and Firefox
Access web-based email	Perform the actual encryption	Changes Firefox to make the process easier