Safe-Guarding Client Information
Basic Data Security Training for Lawyers

Sponsored by the Law Practice Management Committee of The New York State Bar Association

John R. McCarron Jr, Esq.
Partner, Montes & McCarron, PLLC

February 28, 2012

Data Security - Overview

- The most important concept to take away from today – Whether you are a solo or managing partner in a firm of many attorneys: You need a WRITTEN data policy. Commit one to paper and start following it (attempting to follow it).

- What will the data policy apply to?
  - Computers – Laptops & desktops. Office and home use.
  - Mobile devices - Cellphone, Smartphone, Tablet, eReaders, Laptop, Netbook
  - Network use: Wifi in the office, Wifi at home, *Public Wifi*
  - Backup Policy
  - Use of the Cloud

Data Security – Physical Security

- The best data security in the world can be overcome in seconds by these all too common practices:
  - Post it notes with your passwords on them…placed in the following locations:
    - On your monitor, on your laptop, under your keyboard, under your mousepad (that is my favorite)
  - Not locking your doors
  - Leaving laptops, tablets, cell phones in unsecure places
  - Letting children use computers or devices that have your secure data on them.

Encryption

- Encryption explained…
  - What is encryption?
    - The conversion of data into a different form (ciphertext) that cannot easily be read / understood by unauthorized individuals.
    - This sounds much more complicated than it really is. Encryption software will take care of all ‘heavy lifting’. But once employed properly, only the person with the encryption key (password) will be able to access any of the encrypted data.
      - Do not take this lightly…if you lose your password / key you will likely lose access to ALL OF YOUR DATA. There is no “back door” to encryption. Your geeky nephew will likely be of no help. Make a backup of the key and keep it safe.
      - The data encryption employed by my firm will likely withstand decryption attempts by the NSA, FBI, DoD,…

Encryption continued

- What to encrypt…(as much as you can)
  - Your laptop / netbook and even your desktop
    - Mac & PC
      - Software used: Truecrypt, PGP/Symantec, Sophos
    - http://nysbar.com//blogs/TechConnect/2011/05/encrypting_your_hard_drive.html
    - Interesting note – United States Court of Appeals for the 11th Circuit - Nos. 11-12268 & 11-15421, D.C. Docket No. 3:11-mc-00041-LAC. February 23, 2012.
      - Here the Court found that an individual had the right to invoke his 5th Amendment Privilege against self incrimination and not provide a grand jury with his encryption key to decrypt a hard drive where there was allegedly child pornography stored.

Securing The Computer

- Up to date Anti-Virus. Its cheap / free and the baseline protection.
- Password policy. Secure your machine with a strong password and change it often
- Employ encryption!
- Keep your operating system up to date:
  - This includes deploying Windows updates in a reasonable time frame. (They're free and will update themselves if you allow it).
  - Keep your programs up to date.
- Who do you allow to use your computer?

Securing The Computer, continued

- Services such as Lojack for Laptops – helps track down and secure your laptop if stolen.
- Biometric security for login.
- Dual authentication methods (something you know, something you possess)
  - Example – password plus smart card, password plus random key, password plus biometric.
- Facial recognition

Password Management

- Serious password management should be a bedrock principle in your data security policy.
- Do not make all of your passwords the same….even better, do not make them yourself at all. Utilize a random password generator. Choose long passwords (12+ characters, utilizing upper and lower case letters, numbers and symbols where possible)
- Password storage programs such as RoboForm www.roboform.com do a great job of helping create random passwords and manage them. Just make sure your master password is SECURE and CHANGE IT OFTEN.

A word about Portable Drives

- Portable Hard Drives / Thumb drives.
  - A portable hard drive / thumb drive is likely capable of carrying a small to mid sized law firm's ENTIRE client file directory.
    - This should scare you! What happens when you copy all of these files onto an external drive and it gets lost or stolen?
  - Portable drives should never carry client data without being encrypted.
    - There are external storage products that can be purchased which have encryption mechanisms built in.
      - Devices such as "IronKey"(encrypted thumb drive)
      - External Hard drives with encryption and keypad type pin code entry on the actual drive.

Portable Drives…continued

- If you deploy an encryption package on your computer (something such as TrueCrypt), there will be built in controls that if utilized will automatically encrypt data on an external device.
  - Again, an easy and FREE way to get it done.

Dealing with Mobile Devices

- If you have a smartphone (especially if it is synced to your email, contacts, calendar…): EMPLOY A PASSWORD!
  - THIS IS THE MINIMUM "REASONABLE" STEP THAT SHOULD BE TAKEN TO SAFEGUARD THE DATA ON IT (CLIENT DATA?)
- Allowing children to utilize your phone as a gaming device when there is access to client data.
- Employ device tracking technology. In the event that you misplace / lose your phone, most devices now have software built in that allow you to track the phone via GPS, send messages to the phone asking for its safe return, wipe the phone data remotely, or have the phone auto-wipe if the password challenge is not met more than X times in a row.

Mobile Devices Continued

- Apple iOS devices – Find my iPhone/pad
- Blackberry BES remote wipe service
- Android devices have this available as well.

It should be noted that these remote wipe services are often part of a service package (some free with the device), but need to be pro-actively setup. Don’t wait to lose the device!

Also built into Google Apps.

Your Network Connection

- Do you use wireless at home? You likely do. Make sure, at a minimum, you employ an encryption key so that only people who are given the key have access to your network.
  - Better practices include
    - Utilizing newer encryption methodologies such as WPA2 (not the older WEP or WPA which are easily deciphered).
    - Utilizing longer keys
    - Change your keys regularly
    - DO NOT LEAVE THE ROUTER UNSECURED…CHANGE THE DEFAULT PASSWORDS!
    - Hide the SSID (network name) from being broadcast.

Your Network Connection

- Do you utilize wireless in the office?
  - This used to generally be frowned upon but has become a necessary evil in some instances. If you must deploy wireless in your office:
    - Hire the services of an IT professional who can solidify your wireless (and wired) network.
    - Only use professional grade equipment with professional grade encryption.
    - Consider keeping your wireless access as a separate network with no access to client data.
    - Have a separate wireless network for guest access!

Your Network Connection

- Do you utilize public wireless hotspots?
  - Again, more and more we rely upon these. (Internet access in the court houses)
  - Make sure that you employ good local security on your computer.
    - Antivirus & Firewall software (built in firewall is more than sufficient…but make sure you have it turned on)
    - Keep you system secure by keeping it up to date.
  - Most public hotspots are insecure, so make sure that any data you send over it is through a web browser that is encrypted (https) / lock icon in the browser.

Backup Policy

- If you don't backup your data….every day….you are asking for trouble. I would consider it malpractice.
- Backup is easy, and cheap. Choose the right methodology for your needs and size.
  - If you backup to external media….encrypt the backup. Most backup software will allow you to do this automatically.
  - Cloud based backup is growing in popularity.
- The best backup methodology is the one that occurs, automatically, every day, without your intervention, but notifies you if there is a problem. (Set it and forget it).
- Periodically do a TEST RESTORE to see if the backed up data is actually accessible.

The “Cloud”

- The concept of cloud based computing is still the hot topic in 2012. It seems as if the cloud is here to stay and is the direction where all of our data is going.
  - Choose a reputable cloud based provider.
  - Read the service agreement.
  - Where is your data being stored…physically?
  - What does the provider to in the event of a data subpoena
  - Data escrow
    - Coping your data to a 3rd party provider in the even that there is a problem accessing it through the cloud provider.
  - Maybe think about encrypting your data with your own encryption method while storing it at the cloud provider (Dropbox / SecretSync client side encryption)
  - http://nysbar.com/blogs/generalpractice/2011/11/secretsync_-_client-side_encry.html

“Cloud” - continued

- You likely already use the cloud.
  - Ever hear of Hotmail, Gmail, Yahoo Mail,…
- New Cloud Offerings:
  - Salesforce.com, Evernote, Box.net, Google Docs, Google Apps.
- Instead of having to update your software, on your computer(s) each year, updates happen seamlessly and without your intervention. One less thing to worry about. They keep things up to date and secure
- Software is less of a “product” and more of a “service”.

Feel like you are on “Cloud Nine”

- Storing data in the cloud can likely be more secure than storing it locally (proper due diligence required).
  - Software stays up to date.
  - Team of security experts at your cloud provider.
  - Likely uses the same grade encryption as your online banking.
  - Things to look for in your cloud provider:
    - Profitablity / Business model / history
    - ISO 27001 (Information Security Management Systems Standard)
    - Verisign Secured, McAfee Secure, TrustE badges
      - Shows daily security and penetration testing by 3rd party security experts.
      - These icons are likely displayed on login page

More information on Data Security

- General Information:
  - NYSBA Law Practice Management Webpage & Blogs
- Information on Cloud based security
  - Provided by Clio – A cloud based Practice Management Service and NYSBA member benefit.
    - http://www.goclio.com/resources/white_papers/
- Speaker Contact Information:

John R McCarron Jr, Esq
Montes & McCarron, PLLC
68 Main Street
Tuckahoe, New York 10707
(914) 729-1083
jrm@montesmccarron.com