WESTCHESTER LAWYER

WCBA

THE WESTCHESTER COUNTY BAR ASSOCIATION'S MONTHLY MAGAZINE | FEBRUARY 2015 | VOL. 2 | NO. 2

Becoming Proactive About LAW FIRM CYBER SECURITY

... p. 6

Have you renewed your WCBA membership for 2015?

Renew today to keep your member benefits including:

- Monthly *Westchester Lawyer* magazine
- Discounted rates on over 50 CLEs and networking events
- Build your practice by joining our Lawyer Referral Service ... p. 20
- A collective voice at the state and national bar levels and much more ... p. 5

Don't miss out!

- Send in the Express Renewal form ... p. 19,
- Log in to www.wcbany.org, or
- Call Membership Services at: 914-761-3707 ext. 50

In this issue...

BECOMING PROACTIVE ABOUT

LAW FIRM CYBER SECURITY

BY DAVID MENKEN, ESQ.

> "During the early morning hours of June 27, 2014, a hard drive containing backup files for one of the firm's servers was stolen from the locked trunk of an employee's vehicle…. We have confirmed that the hard drive may have contained your name, birthday, Social Security number, driver's license number and contact information, such as your home address, email and phone number."[1]

This breach did not happen to a big-box store. It happened to a criminal defense law firm in California, and the admission was in a letter to an undisclosed number of people, presumably current clients, past clients, employees, and any other individual whose personal information was stored in the stolen hard drive, apparently in unencrypted form.

> "Late Tuesday night Seattle Public Schools learned that a law firm retained by the district to handle a complaint against the district inadvertently sent personally identifiable student information to an individual involved in the case. The district promptly removed the law firm from the case…."[2]

The "personally identifiable information" was apparently sent to just one unauthorized person, but the client was compelled to write to every parent and the law firm was fired.

THESE ARE NOT ISOLATED INCIDENTS. Law firms are increasingly becoming targets of hackers who realize that lawyers, while mostly good at being lawyers, are often terrible at securing their data. The ABA Cybersecurity Legal Task Force estimated that 80 percent of the 100 largest U.S. law firms were subject to successful data breaches by malicious intruders in 2011. That year, the U.S. government labeled New York City's 200 largest law firms "the soft underbelly" of hundreds of corporate clients.[3]

The Ponemon Institute recently estimated that the average cost of a data breach to a company is $3.5 million.[4] Direct costs of a breach include client and

employee notification (plus notification to anyone else whose personal information was compromised, such as individuals disclosed in discovery), investigation expense, crisis management, costs of legal defense, and civil and regulatory liability which can include damages, fines and penalties. Indirect costs can eclipse direct costs when one includes negative publicity, damaged goodwill and eroded client and employee confidence.

LAWYERS ARE OBLIGATED TO PROTECT CONFIDENTIAL INFORMATION

Rules 1.1 and 1.6 of the ABA Model Rules (which have their counterparts in the NY Rules of Professional Conduct) speak directly to confidentiality and clearly confidentiality depends on strong data security.

Rule 1.1, regarding attorney competence, provides that "[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[5] Note 8 to that Rule specifically provides that "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology...."[6]

Rule 1.6(c) provides in pertinent part that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[7]

WHAT IS A DATA BREACH?

New York law defines a data breach as the "unauthorized acquisition ... of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business."[8] "Personal information" is "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person."[9]

Forty-seven states, DC, Guam, Puerto Rico and the Virgin Islands have enacted laws requiring private entities or the government to notify individuals of security breaches involving personal information. Under New York's data breach notification law,[10] even if only one New York resident is to be notified, the breached entity must also inform the Attorney General, the Department of State and the State Police. Plus, if more than 5,000 New York residents are notified at one time the three consumer reporting agencies must also be notified.

(continued on page 12)

Best Practices for Data Security

1. **Encrypt sensitive information**, especially if it contains data protected by Federal (such as HIPAA) or State law, and especially if it can leave the building physically or via an unsecured network. Encryption is a safe harbor under most data breach laws, including New York's.[11]

2. **Conduct a cyber audit**, adopt a written information security program, and plan now on response to a data breach, so that you can respond expeditiously and confidently, and minimize your damages—if it happens to you. That means knowing how to stop the breach, who to call for help, and when and how to notify clients, colleagues, your insurer and the authorities.

3. **Implement a "Bring Your Own Device" policy.** Devices that are not dedicated exclusively to the office should be subject to a "Bring Your Own Device" policy that strictly monitors access to the firm's network and mandates up-to-date security controls.

4. **If you store data in the cloud**, as permitted with conditions by NYSBA Ethics Opinion 842 (9/10/10),[12] take "reasonable care" to ensure that the service you use is secure.

5. **Train and re-train employees** to be cyber-security aware so that they become barriers to entry by crooks and do not intentionally or inadvertently cause the removal of personal information from the workplace or via unsecured wireless connections.

6. **Develop robust disposal policies** of paper and electronic files and also of equipment. Sanitize USB and hard drives before they are discarded. Photocopiers and fax machines have hard drives that contain scans of documents that pass through them, so find out what the copier guy does with the hard drive after the machine is wheeled out the door.

7. **Develop minimum security standards.** If practical, stipulate with opposing counsel to the redaction of personal information (such as social security numbers) that cyber thieves would find more important than the parties. If not possible, stipulate to minimum security standards.

8. **Consider carrying cyber insurance** that will require implementation of best security practices.

(continued from page 7)

There is another important entity to notify of a data breach: the malpractice insurance carrier. There must be few calls less desirable to make than that to the malpractice carrier, putting it on notice of a data breach, especially if the breach was reasonably avoidable.

WHAT LAWYERS NEED TO DO

Risk of a breach can never be entirely prevented, but it can be minimized by exercising proper security precautions. It would be wise, therefore, to consider adopting the steps as "best practices" from a data security perspective listed in the box on page 7.

Safeguarding information simply makes good business sense. When our clients and our colleagues see that we care about the security of their personal information we increase their confidence in us as individuals and as a profession.

ENDNOTES

1 http://www.databreaches.net/law-firm-notifies-employees-after-vendors-server-accessed/.

2 http://www.seattleschools.org/modules/cms/pages.phtml?sessionid=&pageid=320090

3 http://www.sddt.com/reports/article.cfm?RID=955&SourceCode=20130916cwa&_t=Make+sure+your+attorney+protects+your+personal+information#.VH4kI6x0z_Q

4 http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

5 http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence.html.

6 http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1.html. Emphasis added.

7 https://www.google.com/search?sourceid=navclient&aq=&oq=aba+model+rules+1.1+note+8&ie=UTF-8&rlz=1T4GGHP_enUS438US438&q=aba+model+rules+1.6&gs_l=hp..3.41l1066.0.0.2.28194.....0.

8 N.Y. Gen. Bus. Law §899-aa(1)(c).

9 N.Y. Gen. Bus. Law §899-aa(1)(a).

10 N.Y. Gen. Bus. Law §899-aa(8).

11 A NYSBA ethics opinion recently advised that a law firm may give its lawyers remote access to client files, so they can work at home, only if the firm determines that the particular technology used provides reasonable protection to client confidential information or if the client gives informed consent. NYSBA Ethics Opinion 1019 (8/24/14).

12 NYSBA Ethics Opinion 842 (9/10/10).

David Menken, Esq., advises clients on matters involving information technology, privacy and data security at Smith, Buss & Jacobs, LLP. He was founder and first chair of the WCBA's Intelectual Property Committee. He can be reached at dmenken@sbjlaw.com.