CYBER SECURITY INCIDENTS AND DATA BREACHES: IS YOUR LAW FIRM PROTECTED?

By: Jennifer O. Mitchell and Michelle Browning Coughlin, Dinsmore & Shohl LLP

The ever-increasing and alarming number of large companies that have been the recent targets of cyber security attacks, despite their robust security measures, is a wake-up call to every business that stores data electronically. This trend will continue as the sophistication of cyber criminals outpaces modern technological advances. It is not if, but when, the next large data breach will occur. No industry is immune and certain industries, such as health care, are under heightened alert for potential attacks.[1] The theft of confidential information of individuals and the disclosure of private information about companies is a frightening prospect for all lawyers, whose job it is to protect clients' confidential information. Further, the financial costs of cyber attacks to companies can be staggering. The Ponemon Institute's 2014 "Cost of Data Breach Study: Global Analysis" estimates that the average cost of a data breach for a U.S. company is $5.85 million.[2]

Yet, despite these very public cyber security incidents and data breaches, many companies, including law firms, are still not taking adequate steps to protect their own data or the confidential information of their clients. This article outlines some of the key risks to law firms' data, the obligations lawyers have to protect data, and actions that can and should be considered by all law firms as they take steps to comply with their ethical and other obligations with respect to their clients' information.

DATA BREACH RISKS FOR LAW FIRMS

While all entities have some level of risk of cyber attack, law firms are particularly inviting targets for cyber criminals because they maintain a wide array of confidential and sensitive data, both about individuals and large companies.[3] In addition to being targets of cyber attacks, law firms are also subject to the more commonly occurring data breaches that result from loss or theft of laptops, desktops, smart phones, thumb drives, and other devices that carry electronic data. Misconduct or negligent behavior by employees remains a primary risk within a law firm.

With the advent and increased use of cloud computing and other emerging technologies, law firms that utilize cloud services and store their clients' data in cloud-based or other solutions owned by third parties should carefully consider the risks and benefits of doing so and take steps to ensure that cloud and other third party providers adequately secure their data. Law firms should conduct due diligence into cloud and other third party data storage providers and have all required written agreements in place before moving any of their data. A data breach caused by a third party provider could be disastrous to a law firm from both a client relations and financial standpoint.

detection

Data breaches may occur as a result of many system and user weaknesses, including through the improper disposal of electronic devices (including even copy machines), as well as an old-fashioned, low-tech data breach as a result of loss, theft, or improper disposal of paper documents containing confidential information.[4]

THE DUTY TO PROTECT CLIENT INFORMATION IS MULTI-LAYERED

Current Regulatory Requirements

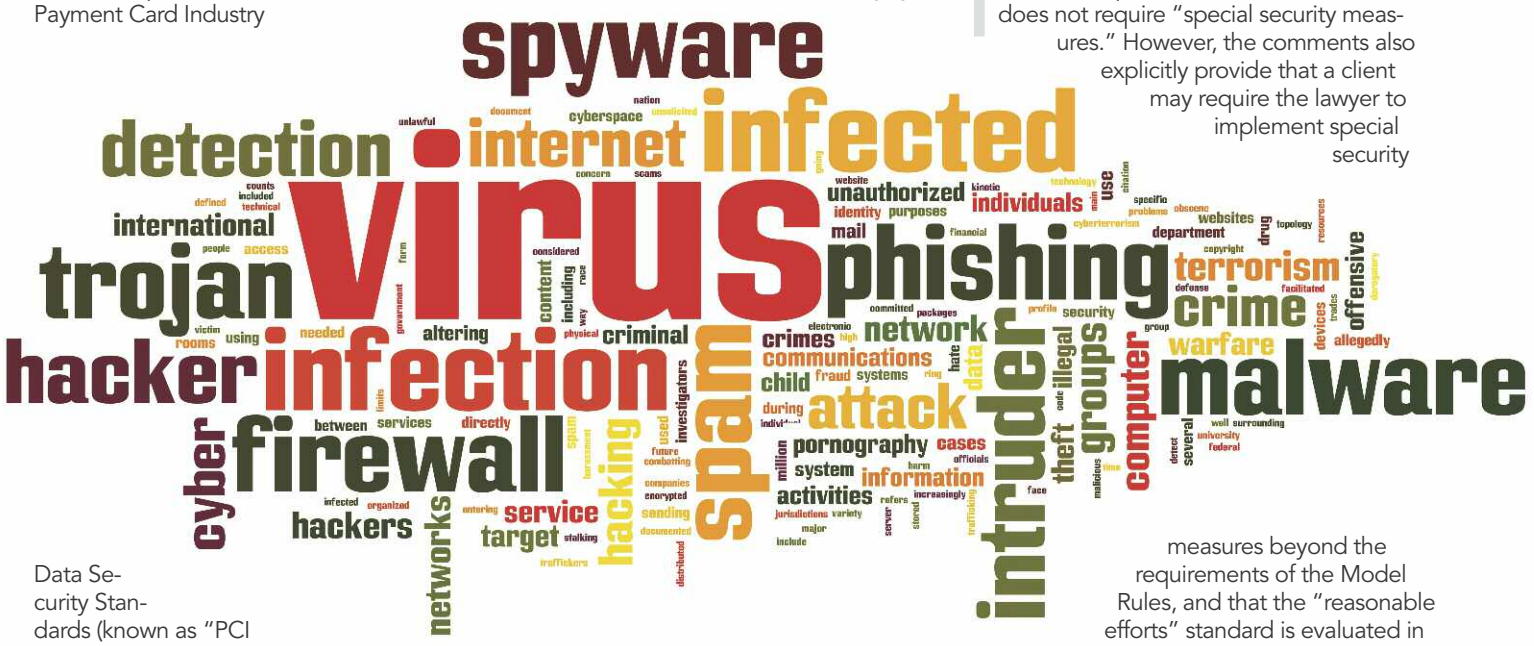
Lawyers are subject to a variety of federal, state, and international regulatory and professional conduct requirements that mandate how lawyers protect client information. Law firms with either lawyers or clients, or both, operating across multiple states or internationally, must contend with the administrative challenges of complying with a multitude of state or international privacy and data security requirements.

hacker

At this time, no general federal breach notification law exists. Recently, however, the Obama Administration proposed the Personal Data Notification & Protection Act, which would serve to create more uniform national privacy and security standards, including breach notification requirements, and attempt to unify the patchwork of state laws that currently exists.[5] Forty-seven states and the District of Columbia have enacted data breach laws impacting businesses, including law firms, within each state. California, in particular, has been seen as on the leading edge of enacting privacy and data security laws, many of which reach well beyond the borders of California. Kentucky was the most recent state to enact a state data breach law, which took effect in July 2014.[6,7] Kentucky's breach notification law requires organizations that are not subject to various other federal privacy laws, like HIPAA or the Gramm-Leach-Bliley Act,[8] to disclose a breach of any Kentucky resident's unencrypted personally identifiable information to the individual if such breach could reasonably cause theft or fraud against the individual.

At a federal level, many law firms are subject to the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as amended by the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act")[9] and the Omnibus Final Rule[10] ("HIPAA"). Lawyers and law firms that use, disclose, maintain or otherwise access protected health information ("PHI") to perform legal services on behalf of their clients are now directly regulated as "business associates."[11] The HIPAA Security Rule sets out specific physical, administrative, and technical safeguards with which lawyers and law firms must comply. In the event that a law firm suffers a data breach involving unsecured PHI, it could be investigated by the Office for Civil Rights, civil and/or

criminal fines could be imposed, and costs associated with required breach notification and mitigation procedures could be incurred, including potential contractual liability to the client whose data was compromised. Additionally, law firms that accept credit card payments may be subject to the financial privacy and data security requirements under the Payment Card Industry Data Security Standards (known as "PCI DSS"), which were established by the major credit card companies and govern the collection, storage, and transmission of credit card data.[12]



Finally, law firms and their clients may be subject to the various international privacy and data security requirements. Many countries outside the United States have taken a more extensive approach to the right to privacy. The European Union, for example, has actively focused on privacy and data security across the EU, including its expansion of EU citizen's privacy rights through the General Data Protection Regulation's inclusion of the "right to be forgotten." Lawyers or clients operating in Canada need to consider Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"), which establishes privacy and data security requirements for private sector businesses; in addition, various provincial statutes have enacted their own privacy and data security requirements. As firms and their clients expand internationally, the privacy and data security requirements also greatly expand.

intruder

ETHICAL OBLIGATIONS TO PROTECT CLIENT DATA

In addition to the more generally applicable state and federal privacy regulations, the ethical issues associated with the security of clients' data, both internally and when stored in the cloud, have been the subject of concern and debate by the legal community for several years. In a December 2010 memorandum from the ABA Standing Committee on Client Protection to the ABA Commission on Ethics 20/20's Working Group on the Implications of New Technologies,[13] the Committee members commented on the Working Group's September 2010 memorandum,[14] saying that "extraordinary diligence in protecting client information" is necessary:

> While there is inherent risk in any form of electronic records storage, whether it is in the "cloud" or lawyer controlled, lawyers who choose to take advantage of these technologies should exercise extraordinary diligence in protecting client information. The Committee believes that the standard should be in line with a best practices standard, and a failure to adhere to that standard that results in the exposure of confidential client information should carry disciplinary consequences.

Despite the Committee's desire to introduce heightened standards, the American Bar Association has taken a more moderate approach. Currently, the Model Rules of Professional Conduct state that a lawyer must implement "reasonable efforts" to protect a client's information and comments to Model Rule 1.6 also state that the duty to prevent unauthorized disclosure does not require "special security measures." However, the comments also explicitly provide that a client may require the lawyer to implement special security measures beyond the requirements of the Model Rules, and that the "reasonable efforts" standard is evaluated in light of factors including the "sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement."

Kentucky's Bar has also provided ethical guidance on the use of cloud-based services. Similar to the commentary to the Model Rules, the KBA Ethics Opinion E-437 states that use of cloud-based services by lawyers is acceptable, but lawyers who do so must use "reasonable care" to ensure confidentiality, and to ensure that client property is safeguarded. As part of this obligation, lawyers are required to "act consistent with [their] duty of competence in selecting and monitoring the providers of cloud-based services," and law firm management must use "reasonable efforts" to ensure any use of cloud-based services is consistent with the ethical obligations.

The KBA Ethics Opinion also requires lawyers to "consult with the client about the use of the cloud if the matter is sufficiently sensitive such that the duty to 'reasonably consult with the client about the means by which the client's objectives are to be accomplished' is implicated."

Again, ethical obligations of law firms operating across multiple states may vary and must be reviewed and policies and procedures developed in accordance with the various ethical and regulatory requirements.

STEPS TO PROTECT LAW FIRM DATA MUST BE SIMILARLY MULTI-LAYERED.

The threats to confidential and sensitive information are numerous, and lawyers' obligations to their clients are significant. Lawyers must develop a proactive and vigilant approach to securing the information entrusted to them. There are a number of steps that lawyers can take to protect their data:

1. Evaluate Cyber Security Budget and IT Staff Resources

Robust cyber security efforts begin with laying the necessary groundwork. Without proper allocation of resources, the ability to take the steps necessary to protect data will be continually hampered. Without proper IT staff – whether hired internally or engaged as a consultant or independent contractor – lawyers are unlikely to have the technological knowledge to implement the proper protections or evaluate the choice of cloud providers or other necessary security vendors. If the budget and staff resources are properly allocated up front, law firms are much more likely to be proactive in developing and keeping current cybersecurity policies and procedures.

2. Conduct a Security Risk Analysis

Conducting a security risk analysis is a necessity in today's cyber security environment. Such an analysis will provide the law firm management – and the IT staff – with a comprehensive review of the firm's IT systems and information that it can use to improve upon any identified security risk areas or vulnerabilities. Risk analyses should be conducted regularly and any time a major change occurs affecting the lawyer's or law firm's administrative, physical, or technical security measures.

3. Encrypt, Encrypt, Encrypt

Encryption is the conversion of data by way of a cryptographic algorithm into a form, called a ciphertext, which is undecipherable for unauthorized individuals. Only an authorize party with a "key" can convert the message back into a decipherable message.[15] Many federal and state laws that regulate the protection of data, including HIPAA and Kentucky's state breach notification law, include safe harbors for encrypted data. The National Institute of Standards and Technology ("NIST") has multiple published white papers on current accepted encryption standards[16] and the costs of encryption technology have decreased significantly over the past several years. As such, encryption is increasingly being considered a reasonable security measure for industries that use or store sensitive consumer information. In fact, in the wake of multiple recent large breaches in the health care sector, federal lawmakers are considering greater encryption requirements under HIPAA.

In order to protect confidential information, and to take advantage of available data breach safe harbors, law firms and lawyers should consider encryption of all mobile devices including laptops, smart phones, and thumb drives (if thumb drives are permitted under your firm's security policies). In the nearly inevitable event that one of these devices is lost or stolen, the fact that the device was encrypted should serve to protect the confidential data contained on the device. Further, if the device is encrypted, the law firm will most likely avoid the difficult position of potentially having to provide notice of a data breach to the affected individuals, clients, the state Attorney General, the Office for Civil Rights, the media, or other parties, depending upon the nature and scope of data contained on the lost or stolen device.

4. Scrutinize use of Cloud-Based Programs and Third-Party Vendors

There are a multitude of cloud-based apps and services that help lawyers and clients communicate with each other more easily, make information more accessible to both lawyers and their clients, help lawyers be more efficient, and even help lawyers and law firms better secure their data. However, there are a number of applications (or "apps") that, while acceptable for personal use, do not pass muster for use in the legal arena. The challenge for many lawyers and law firms is objectively evaluating an app that, while potentially very useful and convenient, simply does not meet the security requirements necessary for use with confidential data.

Law firms should designate an individual or committee with the responsibility to manage third-party vendor contracts, including Business Associate Agreements required under HIPAA, and other cloud-based vendors. All firm staff and lawyers should be trained to consult with that individual or committee before entering into an agreement or taking on an engagement that may require increased data security.

5. Implement and Update Policies and Procedures, including a Data Breach response and Disaster Recovery Plan

Policies and procedures for a law firm need to address: (1) physical security issues, such as properly locked doors or file cabinets, protection of physical files, and proper disposal of confidential information; (2) administrative security issues, such as risk analyses, disaster recovery plans, employee access termination procedures, and other procedural, administrative actions necessary to implement and maintain security measures; and (3) technical security issues, such as use of passwords, access controls, encryption, and audit controls. Basic policies about passwords and password management, proper use of mobile devices, use of VPN encryption for public networks, and other such policies can often be enforced through software deployments by IT staff and are critical protections for sensitive data. Other simple steps, such as preventing physical access to a law firm by non-personnel through properly locked doors and cabinets, require training of lawyers and law firm staff.

In addition, law firms should proactively develop a breach response plan with individual(s) responsible for coordinating analysis of any potential unauthorized access, use, or disclosure of sensitive information, and a disaster recovery plan that will allow for a client's data to be preserved and accessed in the event of a disaster.

6. Consider use of a third-party nationally-certified data center

In some cases, the use of a nationally-certified data center for storage of data is an option to be considered, particularly for a small firm without an IT staff or a firm located entirely in one city. A nationally-certified data center has the advantage of having technological expertise to design and maintain data storage in accordance with the best cybersecurity practices. Furthermore, certified data centers are built in such a way as to protect data during a natural disaster, such as a tornado or flood. However, using a data center means less control over a lawyer's or law firm's data and the potential for data to be inaccessible during service outages. The terms of the contract with the data center must be thorough, and must prevent any situation in which the data could be held "hostage" or released to any third-party without consent, such as under a subpoena issued on the data center.[17]


Jennifer O. Mitchell


Michelle Coughlin

Jennifer Orr Mitchell is a partner in Dinsmore's Health Care Practice Group and leads the firm's HIPAA Privacy and Security practice and initiatives.

Michelle Browning Coughlin is a member of Dinsmore's Intellectual Property Group and has experience assisting clients with privacy and data security compliance issues, including data breach response.

spyware

7. Train all lawyers and law firm personnel

Perhaps most importantly, law firms should implement a training program for lawyers and for all staff who have access to information that is subject to heightened security obligations. Lawyers and law firm staff must understand their ethical and other compliance obligations. Furthermore, they must understand the policies and procedures of the firm itself, what actions must be taken in the event of a potential breach, and who to contact to report actual or potential unauthorized use or disclosure of protected information.

Most lawyers and law firms rely on a multitude of devices, technologies, and apps to stay connected to, and to provide quality and efficient services to, their clients. However, lawyers' confidentiality and data security obligations must remain a top priority for law firms. As the technologies continue to expand and change, lawyers and law firms must continue to adapt and update policies and procedures. While no industry is immune from a cyber threat, law firms can take steps to reduce the threat to their clients', and their own, confidential information.

1 *See* Jennifer Mitchell *et al.*, *A Lesson to be Learned: Electronic Data Breaches Surge in 2014* (Jan. 5, 2015), available at www.dinsmore.com/a-lesson-to-be-learned-electronic-data-breaches-surge-in-2014-01-05-2015/.

2 Study available for download at: www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/.

3 *See, e.g.*, John Simek, & Sharon Nelson, *Preventing Law Firm Data Breaches* 38 American Bar Association Law Practice 1, Preventing, (2012), available at: www.americanbar.org/publications/law_practice_magazine/2012/january_february/hot-buttons.html.

4 *See* Jennifer Mitchell & Stacey Borowicz, *Is Your Photocopier HIPAA Compliant?*, Health Lawyers Weekly, Vol. XI, Issue 49 (Dec. 20, 2013), available at www.dinsmore.com/files/Publication/22326182-b621-4e62-a77b-1e4ed574c3fc/Presentation/PublicationAttachment/902eff8a-0386-4634-91b7-318069a74f17/HLW_122013.pdf.

5 The Obama Administration proposed this Act to Congress on January 12, 2015, encouraging Congress to adopt a federal standard, available at www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf.

6 K.R.S. § 365.732.

7 On March 18, 2015, the Senate Intelligence Committee also approved the Cybersecurity Information Sharing Act of 2015, which encourages companies to voluntarily share information about cyber-threats and authorizes certain defensive measures for private entities' computer networks.

8 The Gramm-Leach-Bliley Act regulates the protection of consumer financial information by financial institutions. 15 U.S.C. § 6801 *et seq.*

9 Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.

10 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5565 (Jan. 25, 2013) (amending 45 C.F.R. 160, 164).

11 See 45 C.F.R. § 160.103; *see e.g.* HHS.gov, Frequently Asked Questions at www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/709.html.

12 Available at www.pcisecuritystandards.org/security_standards/.

13 Memorandum available at www.americanbar.org/content/dam/aba/administrative/ethics_2020/ethics_20_20_comments/abastandingcommitteeonclientprotection_newtechnologiesissuespapers.authcheckdam.pdf.

14 Memorandum available at www.americanbar.org/content/dam/aba/migrated/ethics2020/clientconfidentiality.authcheckdam.pdf.

15 *See* NIST, *Glossary of Key Information Security Terms* (April 25, 2006) available at infohost.nmt.edu/~sfs/Regs/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf.

16 *See, e.g.* NIST, *Recommendation for the Triple Data Encryption Algorithm* (TDEA) Block Cipher (2012), available at csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf.

17 *See* NIST, *Guidelines on Security and Privacy in Public Cloud Computing* (Dec., 2011), available at csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.