THE CYBER THREAT: CLIENTS' INCREASING DEMAND FOR SECURITY AND WHAT IT MEANS FOR LAWYERS

Ellen Murphy[*]

POSTED

Lawyers, you are hereby on notice: cyber threats are real; the legal profession is not exempt (and is, in fact, a direct target). Your duty to protect client confidential information is harder to satisfy than ever before.

INTRODUCTION: THE THREAT

Cyber threats may be the hottest news story no one is actually paying attention to, save the handful of executives and communications teams who must shift to crisis mode, as well as the victim whose privacy has been comprised. Highly public breaches at Target,[1] Home Depot,[2] JP Morgan, Affinity Gaming, Albertsons, UPS, Goodwill, Sony, and White Lodging (a hotel franchise management company serving Hilton, Marriott, Westin and Sheraton)[3] all suggest a growing trend of massive data-sweep attempts across industries. An early February 2015 breach at Anthem, the second largest health insurer in the United States,[4] impacted 80 million clients and revealed a treasure trove of personally identifiable information, including perhaps the most personal of all: social security numbers and birthdates.[5] Initial reports indicate that the breach may be the result of compromised

---

* Adjunct Professor of Law, Wake Forest University School of Law

1. Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG BUS. (Mar. 13, 2014), http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

2. *The Home Depot Reports Findings in Payment Data Breach Investigation*, THE HOME DEPOT (Nov. 6, 2014), https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf.

3. Bill Hardekopf, *The Big Data Breaches of 2014*, FORBES (Jan. 13, 2015, 7:06 PM), http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/.

4. Anna Wilde Mathews & Danny Yadron, *Health Insurer Anthem Hit by Hackers*, WALL ST. J. (Feb. 4, 2015, 9:39 PM), http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720.

5. *Id.*

employee credentials, i.e., stolen passwords retrieved through e-mail phishing schemes.[6]

But if these companies and other victims of cybersecurity theft are not your client, why should you, in your law practice, care? As early as 2009, the FBI warned law firms that they were being targeted through e-mail phishing campaigns.[7] This risk has since increased, and only now are lawyers beginning to take notice. Sadly, however, not notice enough.

THE REGULATORY DEMANDS

Requirements for protecting client information have been near-paramount for lawyers since the *Canons of Ethics* were amended in 1937.[8] Today, absent consent, implied authorization, or a handful of other practically limited exceptions, lawyers have a duty to protect confidential client information "relating to the representation,"[9] a phrase that may cover, practically speaking, any information learned about the matter.[10] Additionally, and at least equally important in the context of cybersecurity, lawyers are required to take "reasonable efforts to prevent the inadvertent or unauthorized disclosures of, or unauthorized access to" this same client information.[11]

While these duties are not new, their application to new technologies and media is, and specific guidance, generally speaking, is inadequate. Nearly two decades ago, the American Bar Association ("ABA") Standing Committee on Ethics and Professionalism addressed the use of third-party information

---

6. Brandon Bailey, *Anthem: Hackers Tried to Breach System as Early as Dec. 10*, U.S. NEWS & WORLD REP. (Feb. 6, 2015, 9:26 PM), http://www.usnews.com/news/business/articles/2015/02/06/anthem-hacker-tried-to-breach-system-as-early-as-dec-10.

7. Joseph M. Burton, *4 Steps to Getting Serious About Law Firm Cybersecurity*, LAW PRACTICE TODAY (Sept. 15, 2014), http://www.lawpracticetoday.org/article/4-steps-getting-serious-law-firm-cybersecurity/.

8. ABA CANONS OF PROF'L ETHICS (1937), *available at* http://www.americanbar.org/content/dam/aba/migrated/cpr/mrpc/Canons_Ethics.authcheckdam.pdf.

9. MODEL RULES OF PROF'L CONDUCT r. 1.6(a) (2014).

10. *See* N.Y. RULES OF PROF'L CONDUCT r. 1.6 (2013), *available at* http://www.nycourts.gov/rules/jointappellate/ny-rules-prof-conduct-1200.pdf (protecting "information gained during or relating to the representation of a client"). *But see* D.C. RULES OF PROF'L CONDUCT r. 1.6(b) (2015), *available at* http://www.dcbar.org/bar-resources/legal-ethics/amended-rules/rule1-06.cfm (protecting only attorney-client privileged information and "other information gained in the professional relationship that the client has requested be held inviolate, or the disclosure of which would be embarrassing, or would be likely to be detrimental, to the client").

11. MODEL RULES OF PROF'L CONDUCT r. 1.6(c) (2014).

technology support personnel,[12] concluding that under Rule 5.3, lawyers must make "reasonable efforts to ensure the protection of its clients' confidentiality"[13] when using such services. The same committee, however, did not comment on lawyers' use of e-mail until 1999, when it concluded that attorneys could use unencrypted e-mail for client communication,[14] reasoning that it offers a "reasonable expectation for privacy."[15] Nearly sixteen years later, it is becoming clearer that the same cannot be said today.

What the ABA has done recently, and perhaps most importantly for practicing lawyers today, is extend the duty of competence[16] to require lawyers to stay "abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."[17]

While it remains to be seen how many jurisdictions will similarly extend this duty[18] and what precisely will be required to satisfy the duty, some states are providing specific guidance focused on the increasing implementation of technology in law practice and

---

12. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 398 (1995).

13. Elizabeth K. Thorp & Kimberly A. Weber, *Recent Opinions from the American Bar Association Standing Committee on Ethics and Professional Responsibility*, 9 GEO. J. LEGAL ETHICS 1009, 1039 (1996).

14. Douglas M. Wade, *Ethical Hazards in a Digital World*, GP SOLO, May/June 2014, at 42, 44, *available at* http://www.americanbar.org/publications/gp_solo/2014/may_june/ethical_hazards_a_digital_world.html.

15. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 413 (1999). Interestingly, the same opinion went on to provide that a lawyer "should consult with the client and follow her instructions . . . as to the mode of transmitting highly sensitive information relating to the client's representation." *Id.* This suggests either that some data may be more in need of protection than others, or perhaps, more likely, that a lawyer should consult with the client on whether e-mail will be an approved method of communication for highly sensitive information.

16. Debra Cassens Weiss, *Lawyers Have Duty to Stay Current on Technology's Risks and Benefits, New Model Ethics Comment Says,* A.B.A. J. (Aug. 6, 2012), http://www.abajournal.com/news/article/lawyers_have_duty_to_stay_current_on_technologys_risks_and_benefits/.

17. MODEL RULES OF PROF'L CONDUCT r. 1.1 cmt. 8 (2014).

18. For example, North Carolina has amended its rules to require lawyers to stay abreast of "the benefits and risks associated with the technology relevant to the lawyer's practice." N.C. RULES OF PROF'L CONDUCT r. 1.1 cmt. 8 (2014), *available at* http://www.ncbar.gov/rules/printrule.asp?id=70. While Florida has not amended its Rule 1.1 accordingly, it provided as early as 2010 that lawyers have an obligation to remain current not only in developments in the law, but also developments in technology that affect the practice of law. Fl. Bar Prof'l Ethics Comm., Advisory Op. 10-2 (2010), http://www.floridabar.org/DIVEXE/RRTFBResources.nsf/Attachments/566CF30AE3172CF385257D5B006CB4D1/$FILE/Ethics%20Opinion%2010-02.pdf?OpenElement. Massachusetts has moved to require an amendment to its Rules in line with the ABA's. Robert Ambrogi, *Mass. Moves to Require Technology Competence for Lawyers*, LAWSITES (July 15, 2013), http://www.lawsitesblog.com/2013/07/mass-moves-to-adopt-duty-of-technology-competence-for-lawyers.html.

the simultaneous increase in cyber threats.[19] But even if these mandatory rules and regulations are not strong enough to change lawyer behavior, the market may be.

CHANGING MARKET DEMANDS

While it may not be immediately obvious why lawyers are potential targets for cyber attacks, consider the vast client information stored on a firm's network: information that personally identifies clients; proprietary corporate information; trade secrets; intellectual property; pending contracts; future IPO dates; investor information; client account numbers, payroll, or other financial information; and even legal work product and strategies.

Even if lawyers do not recognize the threat, clients do. As a result, clients increasingly are not only inquiring about how their information is protected from cyber threats, but they are also requesting proof that adequate protocols are in place and used routinely.[20] Big banks are requiring outside firms to demonstrate that their systems employ "top-tier technologies to detect and deter attacks from hackers,"[21] and some clients are asking firms to complete "60-page questionnaires detailing cybersecurity measures."[22] Others are conducting on-site visits to inspect security for themselves.[23]

THE CHALLENGES IN MEETING THESE DEMANDS

While clients are putting more demands on lawyers to demonstrate that data is protected, they are simultaneously demanding more and better value in legal services, creating competing demands. So while it may be easy to say that "[i]t's just

---

19. Florida has cautioned lawyers to research service providers to ensure adequate security procedures are maintained. Fl. Bar Prof'l Ethics Comm., Advisory Op. 12-3 (2013), http://www.floridabar.org/tfb/TFBETOpin.nsf/b2b76d49e9fd64a5852570050067a7af/4ee735e03432b2f385257bb80050ee57!OpenDocument. Massachusetts requires that a lawyer review the terms of use and data privacy policies of vendors who store confidential client information, as well as take "reasonable efforts" to ensure that the "policies, practices and procedures" are compatible with the lawyer's duty to protect confidential client information, including "examining the provider's existing practices (including data encryption, password protection, and system back ups) and available service history (including reports of known security breaches or 'holes') to reasonably ensure that data stored on the provider's system . . . will not be intentionally or inadvertently disclosed or lost." Mass. Bar Assoc., Ethics Op. 12-03 (2012), http://www.massbar.org/publications/ethics-opinions/2010-2019/2012/opinion-12-03.

20. Matthew Goldstein, *Law Firms Are Pressed on Security for Data*, N.Y. TIMES, Mar. 27, 2014, at B1, *available at* http://dealbook.nytimes.com/2014/03/26/law-firms-scrutinized-as-hacking-increases/.

21. *Id.*

22. *Id.*

23. *Id.*

good business sense"[24] for lawyers to adopt robust security policies and procedures, it is not as easy to implement them. It is resource intensive, in every sense. Fortunately, however, perhaps not nearly as much as you may think.

Many lawyers assume they must understand all of their systems' technological intricacies, large and small, to effectively protect and manage client data. While it may be important to understand a few basics, a lawyer need not get technical to ask the right questions:[25]

- Does our firm have a formal information security protection plan in place, and has it been communicated to all employees?
- Do we have an incident breach policy?
- Do we allow thumb drives for uploading or downloading documents or other items from our company devices?
- Do we permit employees to automatically forward company e-mail to personal e-mail, where it may be more at risk to cyber threats? (E-mail is the primary way hackers get into corporate systems.)[26]
- Do we encrypt all e-mail?
- Do we require secure passwords and frequent password changes?
- Do we prohibit employees from installing their own software on company computers or connecting their own devices to the firm network?[27]
- Do we conduct an annual review of our technology procedures and implement necessary upgrades and refinements?
- Do we conduct security awareness training?
- Do we review our cloud service provider's terms to ensure they are sufficient for us to meet our duties?

Is there a cost associated with these precautions? Without a doubt. Is it large? Yes. But is it doable? Absolutely. There is an abundance of valuable, free information on practice management sites, podcasts, and elsewhere to help lawyers determine how to best

---

24. *Id.* (quoting Mary E. Galligan, an executive in the cyber-risk services division of Deloitte & Touche).

25. *Cyber Risk Management for Lawyers*, LEGAL TALK NETWORK (Sept. 13, 2013), http://legaltalknetwork.com/podcasts/digital-detectives/2013/09/cyber-risk-management-for-lawyers/.

26. *Id.*

27. *Id.*

mitigate the risks.[28] Dedicated cybersecurity experts, in house or outside, can also serve a valuable role. One of the best methods of protection is to have a contractual arrangement in place, in advance of any breach, with a cybersecurity response firm.[29] This will not only help minimize any immediate damage in case of a breach, but can also help mitigate any long-term liabilities that may result in litigation.[30]

The legal profession is not alone in the need to adapt quickly to the new cybersecurity threats; high-profile breaches over the last twelve-plus months show that all businesses (and individuals) that operate online are at risk.[31] Unfortunately, lawyers do not have a reputation for being nimble or quick to adapt.[32] Now is the time to change this perception and the accompanying reality.

There is forward movement; just this week, several banks and big law firms announced the formation of a collaborative body to share "information about threats from hackers, online criminals and even nation states."[33] Service providers also are stepping up. As recently as February 10, 2015, Box[34] announced a new service, Box Enterprise Key Management, which offers "controls for cloud collaboration and file sharing"[35] and is aimed at highly regulated industries,[36] including the legal profession.

---

28. *See, e.g.*, *Help: How Can We Guard Against Cyber-Attacks?,* ATTORNEY AT WORK (Feb. 21, 2013), http://www.attorneyatwork.com/help-how-can-we-guard-against-cyber-attacks/; Stuart A. Krause et al., *Cybersecurity Insurance: It's Not Just for 'The Good Wife',* CORP. COUNSEL (Feb. 5, 2015), http://www.corpcounsel.com/id=1202717092188/Cybersecurity-Insurance-Its-Not-Just-for-The-Good-Wife#ixzz3RkMryqOb; Jody R. Westby, *Cybersecurity & Law Firms: A Business Risk*, LAW PRAC. MAG., July/Aug. 2013, at 46, 47, *available at* http://www.americanbar.org/publications/law_practice_magazine/2013/july-august/cybersecurity-law-firms.html.

29. *Cyber Risk Management for Lawyers*, *supra* note 25.

30. *Id.*

31. *See* Hardekopf, *supra* note 3.

32. *See, e.g.*, George Bellas, *Law as a Commodity,* ATTORNEYS CREATIVE ROUNDTABLE (Mar. 5, 2014), http://www.attorneyscreativeroundtable.com/2014/03/05/law-commodity/; Adrian Dayton, *Of Soccer Balls and Social Media*, MKTG. STRATEGY & THE LAW (Jul. 23, 2014), http://adriandayton.com/2014/07/of-soccer-balls-and-social-media/.

33. Matthew Goldstein, *Wall St. and Law Firms Plan Cooperative Body to Bolster Online Security*, N.Y. TIMES, Feb. 24, 2015, at B7, *available at* http://www.nytimes.com/2015/02/24/business/dealbook/wall-st-and-law-firms-weigh-cooperation-on-cybersecurity.html?ref=dealbook

34. Box is a cloud storage and file-sharing provider, much like Dropbox or Google Docs. *See* https://www.box.com/.

35. Alex Konrad, *Newly-Public Box Unveils Encrypted Key Management To Woo Big Banks As Customers*, FORBES (Feb. 10, 2015), http://www.forbes.com/sites/alexkonrad/2015/02/10/box-unveils-key-management-to-woo-big-banks/.

36. *Id.*

CONCLUSION

With affordable, user-friendly services like Box adapting to changing market needs, lawyers will have fewer excuses if they fail to adapt to their market: clients who want assurances that their data is safe. Given the proliferation of recent cyber attacks, the accompanying media attention, and the repeated warnings, lawyers can no longer argue that they were not aware of the danger.

Consider your client as a business invitee: you have a duty to take reasonable steps to ensure your property is safe. You are hereby on notice that any holes on your land, or in your computer systems, may lead to monetary liability, as well as irreparable reputational harm.