Harvard Journal of Law & Technology
Volume 26, Number 2 Spring 2013

HACKERS, SPIES, AND STOLEN SECRETS: PROTECTING LAW FIRMS FROM DATA THEFT

*Alan W. Ezekiel**

TABLE OF CONTENTS

I. THE GROWING THREAT TO CONFIDENTIAL LEGAL RECORDS

Cyberattacks are increasingly targeting lawyers, and the legal profession must respond more energetically to the threat than it has to date.

Recent years have seen a substantial increase in both hacking and industrial espionage conducted online, at tremendous cost to the vic-

* Harvard Law School, candidate for JD, 2013. The author wishes to thank Jack Landman Goldsmith and Gabriella Blum of the Harvard Law faculty, Kathryn Thompson of the American Bar Association, and Amy Rossignol, Xiang Li, Daniel Robinson, and Michael Adelman of the *Harvard Journal of Law & Technology.*

tims and the national economy.[1] U.S. officials estimate that American companies lost $50 billion in 2009 alone due to cyber-espionage,[2] and some analysts estimate that the worldwide losses due to hacking exceed $1 trillion.[3] The Director of the FBI believes that "the cyber-threat . . . will be the number one threat to the country" in the future, surpassing even terrorism.[4]

The increasing number of data theft and espionage incidents in cyberspace has been widely reported,[5] and law firms have become particularly attractive targets. One data security company reports that 10% of the advanced cyberattacks it investigated in the past 18 months were targeted at law firms.[6]

The risks to law firms are increasing for several reasons. First, computer-savvy intruders are drawn by the quantity and quality of documents available in law offices, routinely including investment plans, negotiation positions, business strategies, descriptions of technical secrets, and due diligence material on financing, transactions, and mergers.[7] Infiltrating attorneys' computer systems is an optimal method of obtaining sensitive material because "[l]aw firms have a tremendous concentration of really critical, private information," explains Bradford Bleier of the FBI's cyber division.[8] Large law firms routinely hold privileged and sensitive documents worth millions of dollars to foreign intelligence services.[9] Second, law firms often have worse data security than their clients. "It's possible the information comes from a very secure source, a company with very good security. Then it goes to a law firm, and who knows what kind of security they are going to have," says Lucy Thompson, chair of the American Bar

1. OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE 1 (2011), *available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

2. Jason Ryan, *US Official Singles Out China, Russia on Cyber-Spying*, ABC NEWS (Nov. 3, 2011, 1:22 PM), http://abcnews.go.com/blogs/politics/2011/11/u-s-takes-hard-line-on-chinese-economic-cyberspying.

3. Kevin Voigt, *Analysis: The Hidden Cost of Cybercrime*, CNN (June 7, 2011, 3:04 AM), http://edition.cnn.com/2011/BUSINESS/06/06/cybercrime.cost/index.html.

4. Jason Ryan, *FBI Director Says Cyberthreat Will Surpass Threat From Terrorists*, ABC NEWS (Jan. 31, 2012, 7:20 PM), http://abcnews.go.com/blogs/politics/2012/01/fbi-director-says-cyberthreat-will-surpass-threat-from-terrorists.

5. *See, e.g.*, Michael Riley & John Walcott, *China-Based Hacking of 760 Companies Shows Cyber Cold War*, BLOOMBERG (Dec. 14, 2011, 8:47 AM), http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html.

6. Kelly Jackson Higgins, *Law Firms Under Siege*, DARK READING (Apr. 6, 2011, 3:47 PM), http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/229401089/law-firms-under-siege.html.

7. JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE, 61–62 (2011).

8. Lolita C. Baldor, *FBI Says Hackers Targeting Law Firms, PR Companies*, SEATTLE TIMES (Nov. 17, 2009, 7:46 AM), http://seattletimes.nwsource.com/html/businesstechnology/2010286161_apushackingfirms.html.

9. BRENNER, *supra* note 7, at 61–62.

Association's Section of Science and Technology Law.[10] Third, data thieves may choose law firms as targets in order to filter out low-value material. Large corporations routinely store so much digital data that an intruder may have trouble sorting the wheat from the chaff; however, a corporation's outside counsel receives and stores a much smaller set of documents, carefully selected for their importance and relevance.[11]

Clients depend upon attorneys to keep their secrets. In order to obtain legal advice, a client will often have to reveal valuable data, future plans, harmful evidence, and embarrassing facts. If the client cannot trust that the information will remain private, he or she may hesitate to obtain legal advice at all. Thus, there is a longstanding professional tradition that people should be able to seek legal advice with confidence that their secrets will not be exposed.[12] Today poor data security is eroding that confidence. In 2011, the hacker collective "Anonymous" stole law firm files concerning the defense of a U.S. Marine accused of misconduct and posted them on the Internet.[13] Chinese hackers attacked several Canadian law firms working on the $40 billion acquisition of the world's largest producer of potash (a valuable agricultural and industrial chemical) and stole strategic data and bidding information.[14] The problem is serious and growing.

This Note considers this problem and proposes some specific measures that the legal profession could deploy to address it. Part II examines the industry-specific challenges that lawyers face when attempting to achieve good data security. Part III discusses the existing statutory and professional rules, showing why they have so far been inadequate to address the problem. Part IV considers possible solutions such as government regulation, liability regimes, security certifications, and changes to professional standards. Part V concludes with recommendations for two changes to professional conduct standards that would help to address the threat.

---

10. Higgins, *supra* note 6; *see also* Geoffrey A. Fowler & Ben Worthen, *Hackers Shift Attacks to Small Firms*, WALL ST. J., July 21, 2011, at A1, *available at* http://online.wsj.com/article/SB10001424052702304567604576454173706460768.html (suggesting that smaller businesses typically have weaker security than major companies).

11. Ed Finkel, *Cyberspace Under Siege*, ABA JOURNAL, Nov. 2010, *available at* http://www.abajournal.com/magazine/article/cyberspace_under_siege.

12. United States v. Grand Jury Investigation, 401 F. Supp. 361, 369 (W.D. Pa. 1975).

13. Chloe Albanesius, *Anonymous Hacks Law Firm Representing Haditha Marine*, PC MAG. (Feb. 6, 2012, 5:45 PM), http://www.pcmag.com/article2/0,2817,2399909,00.asp.

14. Michael A. Riley & Sophia Pearson, *China-Based Hackers Target Law Firms to Get Secret Deal Data*, BLOOMBERG (Jan. 31, 2012, 4:37 PM), http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html.

II. OBSTACLES TO DATA SECURITY AT LAW FIRMS

Data security is famously difficult. The underlying problems are legion and have been widely reported: a battlefield that fundamentally favors attack over defense,[15] the challenges of accurately attributing attacks to their originator,[16] attacks conducted or sponsored by foreign intelligence services[17] with extensive resources and advanced capabilities, and the difficulty of investigating crimes and prosecuting violators across national borders.[18]

Beyond these classic problems, law firms face a number of additional challenges to achieving better data security.

A. Invisibility of the Theft

A major challenge to improving cybersecurity at law firms is the fact that theft of computer data is invisible in the real world.

> Major General William Lord of the air force . . . mentioned [a] massive heist of up to twenty terabytes. To carry this volume of documents in paper form, you'd need a line of moving vans stretching from the Pentagon to the Chinese freighters docked in Baltimore harbor fifty miles away. If the Chinese tried to do that, we'd have the National Guard out in fifteen minutes. But when they did it electronically, hardly anyone noticed.[19]

When a physical item is stolen, the item will thereafter be missing and its absence will likely be noticed. When data is stolen, however, it is merely copied; the original is still there.[20] The invisibility of the loss has several negative implications. It makes detection difficult. It leads to complacency about the threat ("out of sight, out of mind"). It

---

15. David Talbot, *Should We Fire the First Shot in a Cyberwar?*, TECH. REV. (Dec. 14, 2011), http://www.technologyreview.com/web/39315.

16. Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 481–82 (2012).

17. David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SEC. J. 531, 540–41 (2011); Charles Arthur, *Google the Latest Victim of Chinese 'State-sponsored' Cyberwar*, GUARDIAN (Jan. 13, 2010), http://www.guardian.co.uk/technology/2010/jan/14/google-hacking-china-cyberwar.

18. Gerald O'Hara, *Cyber-Espionage: A Growing Threat to the American Economy*, 19 COMMLAW CONSPECTUS 241, 252–53 (2010); Andrew Jacobs, *Follow the Law, China Tells Internet Companies*, N.Y. TIMES (Jan. 14, 2010), http://www.nytimes.com/2010/01/15/world/asia/15beijing.html.

19. BRENNER, *supra* note 7, at 3.

20. *See* Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. ON TELECOMM. & HIGH TECH. L. 359, 379 (2010).

also enables law firms to conceal when they've been victimized. Law firms have strong incentives to conceal breaches,[21] and that naturally leads to systemic underreporting of cyberattacks.[22] It also keeps clients, attorneys, and employees ignorant of the threat, making it difficult to apply corrective measures.[23] Finally, it prevents industry-wide sharing of information that might serve to warn future victims or enable technical collaboration on improved defensive methods.

Cyber victimization presents a classic collective action problem. If companies report intrusions promptly, security researchers can patch the holes and cyberspace becomes safer for everyone.[24] But for any single law firm viewed in isolation, reporting their own victimization seems to present little upside and substantial downside in terms of reputational damage, reduced client confidence, lost business, possible legal liability, and perhaps even emboldening future attackers. A rational cost-benefit analysis may favor silence over disclosure.[25] In fact, some attorneys avoid even *discussing* cyber-threats against their law firms. Two journalists preparing an article for publication described how "[m]ore than a dozen law firms contacted about [a] New York City meeting [with the FBI to discuss hacking attempts against law firms] didn't return telephone calls and e-mails seeking comment."[26] There is a recent S.E.C. guidance requiring disclosure of some cybersecurity incidents,[27] but of course that guidance only applies to publicly held companies, and most law firms are structured as partnerships to which the guidance does not apply.

Most astonishingly, the existing professional responsibility standards generally *do not require any disclosure to the client* when client

---

21. John W. Simek & Sharon D. Nelson, *Preventing Law Firm Data Breaches*, 38 LAW PRAC., Jan.–Feb. 2012, at 22, 22, *available at* http://www.americanbar.org/publications/law_practice_magazine/2012/january_february/hot-buttons.html.

22. Jennifer Smith, *Lawyers Get Vigilant on Cybersecurity*, WALL ST. J., June 25, 2012, at B5, *available at* http://webreprints.djreprints.com/2936070554190.html.

23. Law firms that use cloud-based data storage services can also be on the opposite side of the nondisclosure problem. Most cloud storage agreements do not require the service provider to disclose data breach; thus the law firm itself might be ignorant of the theft of its cloud-stored files. *See* Roland L. Trope & Sarah Jane Hughes, *Red Skies in the Morning — Professional Ethics at the Dawn of Cloud Computing*, 38 WM. MITCHELL L. REV. 111, 219–20 (2011).

24. For example, the "Operation Aurora" attacks in 2009 are inextricably associated in the popular consciousness with Google, but in fact Operation Aurora also struck at least thirty-four other technology companies including Northrop Grumman, Dow Chemical, Adobe, Yahoo, and Symantec. Google was not the only victim, but merely the first one to publicly acknowledge the attack and expose the methods used. Ariana Eunjung Cha & Ellen Nakashima, *Google China Cyberattack Part of Vast Espionage Campaign, Experts Say*, WASH. POST, Jan. 14, 2010, at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html.

25. Benjamin Powell, *Is Cybersecurity a Public Good? Evidence From the Financial Services Industry*, 1 J.L. ECON. & POL'Y 497, 501–02 (2005).

26. Riley & Pearson, *supra* note 14.

27. *SEC Guidance on Disclosing Cybersecurity Risks*, CORPORATE LAW REPORT (Jan. 18, 2012), http://corporatelaw.jdsupra.com/post/16069368719.

information is stolen from a law firm.[28] A law firm can inadequately protect the client's data, get hacked, and neglect to inform the client that data was stolen, all without violating any specific ethical rule.

B. Differential Motivation

Where one party is custodian of the data, but a different party would be harmed by its loss, there is a differential motivation to protect the data.

A correct alignment of motivation is enormously beneficial to data security. In fact it is a key reason that the financial sector's data security is so much stronger than other sectors of the American economy.[29] It is widely understood (as a cultural practice, even where not required by law) that the costs of a successful hacking attack against a financial institution must be paid by the institution itself.[30] Customers are rarely charged for electronic attacks against their accounts; and if they are, the loss is often limited to a nominal amount such as $50.[31] This gives financial institutions a powerful incentive to employ excellent data security measures,[32] and they generally do.[33] For example, banks often require extra security measures for immediate fund transfers[34] and credit card companies proactively monitor customer accounts to detect atypical patterns of spending, promptly calling cuscustomers for confirmation of any questionable transactions.[35]

The financial sector is atypical in this regard, however. In other industries, the stored data may have much less value to the company than it does to the customers. You might care quite a lot whether your browser search history is made public, but the service provider proba-

---

28. *See infra* Part III.C.

29. The financial sector also enjoys statutory and regulatory guidance on data security. *See, e.g.*, the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 (2006 & Supp. V 2012). However, statutory guidance alone cannot explain the strong data security practices in the financial sector relative to other industries. The health care sector, for example, likewise has statutory guidance. *See* Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8334, 8334 (Feb. 20, 2003) (45 C.F.R. pts. 160, 162, 164), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf. However, it lacks the strong industry-wide practice standards that are informally but broadly enforced within the financial sector, such as STATEMENT ON AUDITING STANDARDS NO. 70 (1992) or STATEMENT ON STANDARDS FOR ATTESTATION ENGAGEMENTS NO. 16 (2010).

30. Erin Fonté, *Who Should Pay the Price for Identity Theft?*, FED. LAW., Sept. 2007, at 24, 25.

31. *See, e.g.*, 15 U.S.C. § 1643 (2006) (a)(1)(B).

32. Soghoian, *supra* note 20 at 378.

33. Powell, *supra* note 25, at 502–04.

34. In *Shames-Yeakel v. Citizens Fin. Bank*, a bank was sued for allowing a fraudulent transaction without extra security steps such as two-factor authentication, and the court denied the bank's motion for summary judgment. 677 F. Supp. 2d 994, 1000, 1009 (N.D. Ill. 2009).

35. Daniel Bukszpan, *How Credit Card Companies Detect Fraud*, CNBC (Mar. 30, 2012, 5:14 PM), http://www.cnbc.com/id/46907307/How_Credit_Card_Companies_Detect_Fraud.

bly does not care at all, except insofar as it might suffer negative secondary effects (such as bad publicity or the loss of your business). The service provider has control of the record, but you care much more whether it gets stolen.

Law firms likewise have differential motivations to protect client data. The client is sharing secrets — embarrassing depictions of their dysfunctional married life, the details of an alleged crime, diagrams of their newest patentable invention, or plans for a corporate acquisition — which have great value to the client, but are just routine everyday work to the attorney. For some clients, such as high-tech startups or merger participants, the secrets might be worth a large portion of their company's total value. The damage to the law firm, however, is a much smaller number — namely, that fraction of the client's losses that would hypothetically have been spent on future legal fees.[36] As a result, the client will usually have a much stronger incentive to protect their own private information than the law firm does, which perhaps explains why "[l]awyers haven't been as diligent with security as some of the institutions that gave them information."[37]

C. Security Is Expensive and Inconvenient

Strong security is a hassle. It means choosing different passwords (each too long to remember easily) for all your various accounts and websites, and encrypting your files with key phrases that are long and unintuitive.[38] It means not carrying critical data on your mobile device, which sometimes deprives you of data access that would improve your efficiency and productivity.[39] It means throwing away all your thumb drives.[40] It means that you sometimes cannot send sensitive documents through e-mail, and must look for other (slower, more expensive, less convenient) ways to transmit them securely wherever

---

36. The damages to the law firm could be greater if the client becomes aware of the breach. In that case the firm might suffer reputational damage and the loss of the client's future business. However, it is not very likely that the client will independently learn of the breach, as discussed *supra* Part II.A and *infra* Part IV.B.

37. Finkel, *supra* note 11 (quoting attorney Marc Zwillinger).

38. *See, e.g.*, Dan Pinnington, *Don't Be Passé With Passwords: Best Practices for Staying Safe*, 31 L. PRAC., July–Aug. 2005, at 27, 27, *available at* http://www.americanbar.org/publications/law_practice_home/law_practice_archive/lpm_magazine_articles_v31is5an18.html; David Coursey, *Study: Hacking Passwords Easy As 123456*, PCWORLD (Jan. 21, 2010, 1:00 PM), http://www.pcworld.com/article/187354/Study_Hacking_Passwords_Easy_As_123456.html.

39. *See, e.g.*, Kevin Johnson, *CIOs Must Address The Growing Mobile Device Security Threat*, FORBES (Aug. 16, 2012, 7:55 PM), http://www.forbes.com/sites/ciocentral/2012/08/16/cios-must-address-the-growing-mobile-device-security-threat.

40. Thumb drives are a common vector for malware transmission, particularly for systems insulated from public networks. *See*, Gregg Keizer, *1-in-4 Worms Spread Through Infected USB Devices*, COMPUTERWORLD (Aug. 26, 2010, 3:35 PM), http://www.computerworld.com/s/article/9182119/1_in_4_worms_spread_through_infected_USB_devices.

they need to go.[41] It means hiring skilled IT staff, purchasing security software, training employees, setting policies, and monitoring compliance.

As businesses strengthen their security, cyber-intruders are increasingly focusing instead on their law firms, which often have all the important data but much weaker security precautions.[42] This is especially true when the law firm is substantially smaller than the client, and thus less capable of handling the cyber-threats the client's data will likely attract. A law firm may lack the resources, the technical knowledge, or the will to consistently keep its clients' data adequately protected. Even in organizations much more structured and disciplined than law firms, the day-to-day hassle tends to erode good security practices over time.[43] "When convenience butts heads with security, convenience wins."[44]

D. Cultural Obstacles

Law firms have traditionally been organized as partnerships in which the partners are co-owners of the firm.[45] In an environment where so many people are "bosses," it is socially and culturally difficult to impose policies (such as good security practices) that are troublesome, inefficient, and annoying on a day-to-day basis. Many partners will lack an interest in data security, or will have a determined preference for the way they have always done things in the past.[46] Furthermore, professional standards generally do not allow anyone but attorneys to be partners in law firms[47] or to hold any managerial authority,[48] which means that the head of the IT department, charged with maintaining data security, is almost certainly outranked by all the senior attorneys upon whom he or she is trying to impose these cumbersome security practices.

---

41. *See* David Ma, *Internet E-mail Is Not Secure*, TECHBLAWG (Jan. 27, 2009), http://techblawg.ca/2009/01/27/internet-e-mail-is-not-secure/; *If You Want Privacy, Don't Count on Email. Here's Why.*, NOLO, http://www.nolo.com/legal-encyclopedia/email-privacy-29610.html (last visited May 9, 2013).

42. Seth L. Laver, *Fortifying the Law Firm: Understanding and Protecting Against Cyber Risk*, FOR THE DEFENSE, July 2012, at 46, 46.

43. The U.S. military, for example, has been unable to keep its networks secure. *See* BRENNER, *supra* note 7, at 80–85, 88–91.

44. *Id.* at 38.

45. Mark Rosencrantz, *You Wanna Do What? Attorneys Organizing as Limited Liability Partnerships and Companies: An Economic Analysis*, 19 SEATTLE U. L. REV. 349, 354, 369–70 (1996).

46. BRENNER, *supra* note 7, at 61.

47. MODEL RULES OF PROF'L CONDUCT R. 5.4(b) (1983). This rule has been the subject of debate, but proposals to relax it were recently shelved. James Podgers, *Summer Job: Ethics 20/20 Commission Shelves Nonlawyer Ownership, Focuses on Other Proposals*, ABA JOURNAL, June 2012, at 27, 27, *available at* http://www.abajournal.com/magazine/article/summer_job_ethics_20_20_commission_shelves_nonlawyer_ownership.

48. MODEL RULES OF PROF'L CONDUCT R. 5.4(d)(2) (1983).

III. CURRENT RULES ON DATA SECURITY

A. Legislation

Although federal and state legislatures have passed numerous laws related to online privacy, these laws generally do not cover client files stored by law firms.

Most privacy-protection laws are tightly focused on "personal information" (sometimes called "personally identifiable information" or "PII"), which is usually defined as some combination of an individual's name, driver's license number, social security number, a financial account such as a credit card or bank account number, or other similar functional identifiers.[49] States often require PII to be stored or handled in certain ways, such as requiring encryption when PII is transmitted across public networks[50] or stored on mobile devices.[51] When PII is stolen, forty-five states require the custodian to disclose the breach to the affected individuals, or to the state.[52]

However, most law-office files are not PII. Despite the nomenclature, these privacy protection laws are not actually designed to protect privacy, but rather to combat economically motivated fraud and identity theft. The definition of PII reflects that goal, which is why financial account numbers are protected while so many other types of potentially private data are not.[53]

A law office's *billing records*, if they contain the financial account numbers of individuals, are PII; thus the attorney must give notice if such records are stolen. However, the *client files* — the records of the client's newest invention, planned corporate merger, premarital agreement, or trial strategy — are not PII. These legal matters are potentially much more important to the client's welfare and sense of privacy than any credit card number will ever be, but they are not covered by most states' privacy and disclosure laws.

There seem to be few statutory requirements for the storage and protection of client files, or for law firms to disclose when client files are stolen.

---

49. Brandon Faulkner, *Hacking into Data Breach Notification Laws*, 59 FLA. L. REV. 1097, 1105–06 (2007); *see, e.g.*, ARIZ. REV. STAT. ANN. § 44-7501(L)(6) (2007); 201 MASS. CODE REGS. § 17.02 (2013).

50. 201 MASS. CODE REGS. § 17.04(3) (2013).

51. *Id.* at § 17.04(5).

52. VIRGINIA A. JONES, REQUIREMENTS FOR PERSONAL INFORMATION PROTECTION, PART 2: U.S. STATE LAWS, ARMA INTERNATIONAL EDUCATIONAL FOUNDATION, 11 (Nov. 2009), *available at* http://www.armaedfoundation.org/pdfs/Requirements_for_Personal_Information_US_States.pdf.

53. *See* Soghoian, *supra* note 20, at 379.

B. Professional Standards on Safeguarding Client Information

Generally lawyers are required by professional standards to keep client information confidential. However, those rules tend to focus on intentional revelations by the attorney and often have glaring blind spots where the protection of stored electronic data is concerned.

Most state bar rules contain a broad prohibition on attorneys intentionally disclosing client information, followed by several subsections that describe the rare circumstances under which intentional disclosure is allowed or required.[54] In many cases attorneys are also responsible for the intentional acts of their office staff, as in New York where lawyers must "exercise reasonable care to prevent the lawyer's employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidential information of a client . . . ."[55] However, mere carelessness or inadequate protective measures are not generally addressed. Even the simplest protective steps, such as having a firewall installed on a file server, are not explicitly required.

On the contrary, the rules on electronically stored records almost all relate to preserving the data for the client, rather than protecting it from theft. In Maine, for example, "important correspondence and documents created by the attorney on the client's behalf [must] be retained in a way that insures that the client and the attorney are able to access these records in the future."[56] New York lawyers must "make certain that the new storage means to be used safeguards the records from inadvertent destruction," but the rule says nothing about safeguarding from theft.[57] Florida is even more explicit: "[T]he main consideration in [electronic] file storage is that the appropriate documents be maintained, not necessarily the method by which they are stored."[58]

Some states also explicitly allow attorneys to store their electronic records in the cloud. Obviously this involves placing the data in the custody of for-profit companies outside the lawyer-client relationship, and then transmitting the data over the Internet each time it is accessed by the attorney. These rules generally require the law firms to take "reasonable efforts,"[59] "reasonable steps,"[60] or "reasonable pre-

54. *See, e.g.*, Cal. Rules of Prof'l Conduct, Rule 3-100(A) (2004); Minn. Rules of Prof'l Conduct, Rule 1.6 (2005).

55. N.Y. Rules of Prof'l Conduct, Rule 1.6(C) (2009).

56. Me. Prof'l Ethics Comm'n of the Bd. of Overseers of the Bar, Op. 183 (2004) (discussing lawyer's obligations concerning the manner of retention of client and law office records).

57. N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 680 (1996) (discussing record retention by electronic means).

58. Prof'l Ethics of the Fla. Bar, Op. 06-1 (2006).

59. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 95-398 (1995).

cautions"[61] to avoid unauthorized disclosure, but are unspecific about what such precautions might entail. One rule demands that the precautions taken must "meet[] industry standards,"[62] but is unfortunately vague about whether it refers to the standards of the *legal* industry or those of the *Internet data storage* industry.

Viewed one way, these results are quite reasonable. Until recently, the rules of professional conduct made attorneys liable for their own conduct, and for the conduct of people under their control, such as office staff, but not for the criminal actions of third parties.[63]

This view — that attorneys are not responsible for violations of client privacy that flow from criminal misconduct by third parties — may have been informed by the evolution of legal standards regarding the use of mobile phones. Several state rules of professional conduct advanced in the early 1990s suggested that attorneys might violate ethical standards by discussing private client information on mobile phones because outsiders could overhear the conversations.[64] By the late 1990s and early 2000s, however, the professional rules were shifting to the view that the Electronic Communications Privacy Act (which criminalized interception of wireless telephone conversations)[65] created a reasonable expectation of privacy on a mobile phone; and thus the attorney could discuss client matters on a mobile phone without violating any ethical standards.[66] The fact that an out-

60. State Bar of Ariz. Comm. on Rules of Prof'l Conduct, Formal Op. 05-04 (2005); 21 Law. Man. On Prof. Conduct 384 (ABA/BNA).

61. State Bar of Nev. Standing Comm. on Ethics & Prof'l Responsibility, Formal Op. 33 (2006); 22 Laws. Man. on Prof. Conduct 80 (ABA/BNA).

62. Mo. Bar Legal Ethics Council, Informal Op. 2006-0092 (2007).

63. The ABA model rules were fairly typical in this regard. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 18 (July 2012) ("A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision."). The Rules were revised in August 2012 to include liability for the criminal actions of third parties. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 18.

64. *See, e.g.*, Ill. State Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 90-7 (1990) ("Inasmuch as [mobile telephone conversations] will not be treated as confidential and may result in the loss of the attorney-client privilege, a lawyer should not use a cordless or mobile telephone when speaking to a client about confidential matters."); Mass. Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 94-5 (1994) ("[A]ny nontrivial risk that [confidential] information may be overheard [on a cellular telephone requires client consent]."); N.H. Bar Ass'n Ethics Comm., Formal Op. 1991-92/6 (1992) ("If a lawyer desires to use mobile communications to communicate . . . about a client's representation, the lawyer must first disclose to the client that the mobile communication may not be secure . . . .").

65. *See* 18 U.S.C. § 2511 (2006 & Supp. V 2012) ("Interception and disclosure of wire, oral, or electronic communications prohibited").

66. *See* State Bar of Ariz. Comm. on Rules of Prof'l Conduct, Formal Op. 95-11 (1995) ("[T]he time has not yet come when a lawyer's mere use of a cellular phone to communicate with the client . . . constitutes an ethical breach."); Del. State Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 2001-2 (2001) (finding that use of a mobile phone is permissible unless "extraordinary circumstances" make disclosure likely); Minn. Law. Prof'l Resp. Bd., Op. 19

sider might be able to overhear the conversation was irrelevant because the outsider would thereby be committing a felony.

One could easily analogize to the electronic storage of client records. A hacker would be committing a felonious violation of the Computer Fraud and Abuse Act by accessing client records without authorization,[67] and therefore state bar associations might see no professional violation by an attorney who fails to prevent such access. But should the fact that hacking is illegal excuse an attorney who fails to take even the most basic security precautions in an era of widespread data theft?

Fortunately, the situation is improving. A few states have adopted more modern standards for protection of electronic client files. Lawyers in New Jersey, for example, may store files in digital format, but must use "sound professional judgment on the steps necessary to secure client confidences against foreseeable attempts at unauthorized access."[68] Recently the American Bar Association ("ABA") likewise updated its model rules of professional responsibility,[69] adding (among other things) a new section requiring 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."[70]

C. Professional Standards on Disclosure of Data Theft

Once a theft of client data has occurred, professional standards surprisingly do not require any disclosure to the client. Attorneys must "promptly inform the client of any decision or circumstance with respect to which the client's informed consent . . . is required,"[71] but of course consent is not required to be the victim of a theft. The official comments further clarify that the rule is concerned with client participation in decision-making, such as the selection of legal strategies or whether to accept a settlement offer or plea bargain.[72] In fact, the comments to the ABA model rules explicitly sidestep any attorney responsibility for notification of data loss with a blunt statement that

(1999) (holding that use of digital cordless and cellular phones or e-mail, even unencrypted, is permissible).

67. *See* 18 U.S.C. § 1030(a)(2)(C) (2006 & Supp. V 2012).

68. N.J. Advisory Comm. on Prof'l Ethics, Formal Op. 701 (2006); *see* 22 Law. Man. of Prof. Conduct 236 (2006).

69. *See* Sean Doherty, *ABA Adopts Ethics Policy on Lawyers' Use of Technology*, L. TECH. NEWS (Aug. 8, 2012), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202566577730&ABA_Adopts_Ethics_Policy_on_Lawyers_Use_of_Technology.

70. MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (2012).

71. MODEL RULES OF PROF'L CONDUCT R. 1.4 (1983).

72. *See id.* at CMTS. 1–3, 5 (1983).

"notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules."[73]

A law office that suffers a data breach and the loss of confidential client information can, without violating any specific ethical standard, withhold all knowledge of the breach from the client whose data was stolen. For obvious reasons, it is difficult to collect meaningful statistics about the frequency of such occurrences, but anecdotal evidence suggests that attorneys do sometimes withhold such information from their clients.[74]

IV. METHODS OF IMPROVING CYBERSECURITY AT LAW FIRMS

This Part will discuss and critique several possible methods to address the problem of cyber-vulnerability at law firms. Some of the methods discussed are generally applicable (e.g., government regulation) while others are more tightly focused on the legal field (e.g., professional standards).

A. Government-Mandated Defensive Measures

Many of the vulnerabilities that hackers exploit arise due to inadequate care on the part of computer system administrators.[75] At first glance it might seem that the government could simply mandate the measures necessary to close the obvious holes, thereby substantially reducing the vulnerability of our computer networks. Unfortunately, that approach raises a number of serious problems.

First, the threat environment is extremely fast-moving. Maintaining security requires flexibility and frequent updates to address rapidly evolving threats. In 2012, for example, Microsoft's Windows Update utility distributed over 300 different patches and updates, of which a substantial majority were related to security threats.[76] It is unclear whether a government regulatory agency could operate at such a pace. Critics suggest that government-designed technical

---

73. MODEL RULES OF PROF'L CONDUCT R. 1.6 CMT. 18 (2003).

74. *See, e.g.*, Alan Paller, *Conversations on Cybersecurity: The Trouble with China, Part 1*, FORBES (Jan. 31, 2012, 2:36 PM), http://www.forbes.com/sites/ciocentral/2012/01/31/conversations-on-cybersecurity-the-trouble-with-china-part-1.

75. For example, one study showed that 75% of all cyberattacks exploiting software vulnerabilities were targeted at vulnerabilities for which a remedial software patch had been available for three months or longer. *See* VERIZON BUSINESS RISK TEAM, 2008 DATA BREACH INVESTIGATIONS REPORT 15 (2008), http://www.verizonenterprise.com/resources/security/databreachreport.pdf.

76. *See Description of Software Update Services and Windows Server Update Services Changes in Content for 2012*, MICROSOFT SUPPORT, http://support.microsoft.com/kb/2800436 (last visited May 9, 2013). Note that the list oddly misclassifies as "non-security content" many updates that are clearly related to security, such as KB2785605, KB2758994, KB2755399, KB2770041, KB2736233, KB2695962, KB2647518, and multiple updates under KB890830 and KB931125. *Id.*

standards would be obsolete the day they were passed, and would be too rigid to change as quickly as needed.[77]

Andrew McLaughlin suggests a second reason for concern: having a nation's offensive and defensive cyber-operations directed by the same organization creates decisional conflicts.[78] Imagine that a government researcher discovers a zero-day exploit.[79] Such an exploit could be used two ways: offensively, to penetrate foreign systems and steal their data, or defensively, by developing a fix and patching domestic computer systems. Government intelligence agencies, argues McLaughlin, are far more likely to prioritize offensive uses first, and to continue using the exploit offensively until somebody else discovers and publicizes it.[80] For that reason, a robust cyber-defense organization needs to do its work (and be led) separately from teams responresponsible for conducting offensive cyber-operations.[81]

Third, the notion of government-mandated security measures may implicate privacy and civil liberty concerns. By their nature, defensive software programs generally have substantial oversight and control over the computer, which is the reason malware often disguises itself as security software.[82] If the government designs or produces the security software, then users must trust government-provided programs with their personal data. Not all users will be comfortable with that

---

77. *See* Joel Brenner, Of Counsel, Cooley LLP, Address at Harvard Law School National and International Security Law class (Oct. 17, 2011); e-mail from Joel Brenner, Of Counsel, Cooley LLP, to the author (Feb. 6, 2013, 21:14 EST) (on file with author); *see also* BRENNER, *supra* note 7, at 223–24.

78. *See* Andrew McLaughlin, Address at the Radcliffe Institute for Advanced Study Cybersecurity Symposium (May 19, 2011); *see also* e-mail from Andrew McLaughlin, to Caroline Nolan, Associate Director, Berkman Center (Feb. 6, 2013, 20:32 EST) (on file with author) [hereinafter McLaughlin e-mail].

79. A "zero-day exploit" refers to a newly discovered cybersecurity vulnerability. Since defenders cannot patch a vulnerability that they have not yet discovered, a newly discovered security flaw can often be used on "day zero" (i.e., the first time that particular flaw has ever been exploited) to penetrate even a well-maintained and otherwise secure computer system. Once the vulnerability becomes widely known, however, it will soon be patched. Zero-day exploits thus have substantial value as long as they are kept secret, but their value drops precipitously soon after they are publicized. Their value can even be monetized. *See* Andy Greenberg, *Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits*, FORBES, (Mar. 23, 2012, 9:43 AM), http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits.

80. McLaughlin e-mail, *supra* note 78.

81. McLaughlin believes that:

> it's possible (indeed, even desirable) for a cybersecurity organization to do both offense and defense, because the defensive team can get uniquely valuable information from the offensive team, and vice versa, but it has to keep the functions separate, bound by a serious and difficult process of evaluating and balancing the competing interests in either direction.

McLaughlin e-mail, *supra* note 78.

82. *See* SYMANTEC, SYMANTEC REPORT ON ROGUE SECURITY SOFTWARE 1 (2009), *available at* http://eval.symantec.com/mktginfo/enterprise/white_papers/b-symc_report_on_rogue_security_software_exec_summary_20326021.en-us.pdf.

requirement, and it obviously raises particular concerns among attorneys, who may represent clients in civil or criminal litigation against the government.

Of course, these concerns could be addressed by crafting less-specific legislation that merely establishes broad standards ("shall take reasonable steps to . . .") but does not seek to impose specific technological solutions. Such legislation would face two challenges. First, absent statutory or regulatory guidance, it is unclear how such a measure would be enforced. Who would decide what measures are "reasonable?" Second, governments have shown little enthusiasm for establishing meaningful broad standards for cybersecurity. The 112th Congress, for example, was unable even to pass the Cybersecurity Act of 2012, which would have required additional cybersecurity measures for crucial infrastructure businesses (such as utility companies) whose failure might result in "catastrophic economic damage."[83] It thus seems unwise for the legal profession to await government direction before protecting client files.

B. Liability Regimes and Private Causes of Action

Liability is one of the legal levers used to encourage preventive behaviors. In theory, if a lawsuit can collect a reasonably predictable award for a harm (in this case, a cyber-breach and loss of data), then insurance companies will sell insurance against such lawsuits. The need to price such policies would motivate insurance companies to establish actuarial standards that measure risk, and those standards would guide the development of preventive measures, similar to the way in which insurance companies encourage the installation of smoke detectors in private homes by offering an insurance discount when one is installed. Such guidance, the theory goes, tends to improve preventive measures and reduce harms.

Some academics are exploring the use of liability levers to improve cybersecurity in this way.[84] The problems are enormous, however, and may even be insurmountable.

First, cyber-theft often goes undetected. The invisibility of the wrongful act and the lack of easy detection undercuts the entire liability regime. Absent knowledge that the wrong has occurred, no suit can be brought.

---

83. Cybersecurity Act of 2012, S. 2105, 112th Cong., § 103 (b)(1)(C)(ii); *See* Eric Engleman, *Cybersecurity Bill Killed, Paving Way for Executive Order*, BLOOMBERG (Nov. 14, 2012, 7:40 PM), http://www.bloomberg.com/news/2012-11-15/cybersecurity-bill-killed-paving-way-for-executive-order.html.

84. *See, e.g.*, Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 265 (2005); Vincent R. Johnson, *Data Security and Tort Liability*, 11 J. INTERNET L., Jan. 2008, at 22, 30; Stevan D. Mitchell & Elizabeth A. Banker, *Private Intrusion Response*, 11 HARV. J.L. & TECH. 699, 720 (1998).

Second, even if the cyber-breach is detected, it will almost certainly be detected by the prospective defendant, the attacked law firm. The prospective plaintiff, the client, is unlikely to know about it unless the defendant reports it — something the defendant has an obvious disincentive to do in a liability-based regime. As discussed above, the poor reporting of cyber-breaches is already harming our defensive landscape. Costly liability penalties would add even more reasons for companies to conceal cyberattacks, which seems perverse.

Third, it is difficult to prove and quantify the harm. Even if the breach is detected, it may not be clear what was stolen, or how much it was worth, and it probably will not be clear who stole it.[85] Breaches are committed for a wide variety of reasons, and calculating the monetary harm of a data loss is going to be dependent upon who stole the data and what they plan to do with it. In fact, this problem is so severe that some appellate courts have dismissed such cases outright, finding a lack of standing to bring suit because the harm "is dependent on entirely speculative, future actions of an unknown third-party."[86] When the harms are incalculable the legal system sometimes turns to statutory damages, but statutory damages fail to account for the actual value of the harm. The secret formula for Coca-Cola is worth enormously more than a family recipe for chocolate chip cookies,[87] and it deserves a lot more protection. A regime of statutory damages might establish a "floor" level of data protection for personal data with nominal or dignitary value, but offers little potential for addressing the problem of industrial cyber-espionage, which causes far greater economic harm.

Finally, long delays between the breach and the harm are routine.[88] If the theft involves corporate secrets, the victim may not even realize what happened until years later, when a foreign competitor is discovered to have made use of the stolen data. That puts the plaintiff in a position of waiting, perhaps for years, to see what the eventual harms will be. The plaintiff must then try to prove causation between the data breach and the harm — and that is likely to be impossible. How can the plaintiff establish that the harm flowed from one specific alleged breach years ago, and not from some other lapse or breach?

Combined, these problems are so severe as to cast doubt on liability regimes as practical mechanisms for improving cybersecurity.

---

85. Kesan & Hayes, *supra* note 16, at 481–82.

86. Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011).

87. The secret formula for Coca-Cola is thought to be "worth many billions of dollars." Gene Quinn, *Vault with Coca-Cola Trade Secret Formula on Public Display*, IP WATCHDOG (Jan. 6, 2012, 8:10 AM), http://www.ipwatchdog.com/2012/01/06/vault-with-coca-cola-trade-secret-formula-on-public-display/id=21588. A home baker's recipe for chocolate chip cookies presumably has a commercial value near $0.

88. CHUCK EASTTOM, COMPUTER SECURITY FUNDAMENTALS 136 (2d ed. 2012).

C. Professional Standards Requiring Basic Security Practices

There is enormous room for improvement in the professional responsibility rules surrounding storage of electronic data. Most state bar rules do not discuss secure storage of client data. This is a substantial oversight in an increasingly digital world, where more and more data is on the Internet and thus vulnerable to hacking.

Law firms cannot prevent all hacking, but 96% of hacking attacks employ simple techniques, and 97% of attacks could be blocked by common security practices that are within the reach even of small law firms and solo practitioners.[89] These common practices include the use of current virus scanners and firewalls, installing patches and updates, using cryptographically strong passwords, avoiding risky software downloads from the Internet, replacing the default passwords on network hardware, and training employees to recognize deception ("phishing") attacks.[90] Basic security measures should be a professional requirement for any attorney who stores sensitive client data on an Internet-connected computer.

D. Professional Standards Requiring Disclosure of Data Theft

Concealing or failing to disclose the theft of a client's data should be viewed as an ethical violation. Disclosure is essential not only because the client has a legitimate interest in knowing when confidential data has been stolen but also because the client may be able to mitigate the damage, for example by changing strategies, technologies, or product timing, or by filing patents or copyrights in the jurisdiction from which the breach originated. The client also has a better chance than the attorney of identifying the perpetrator, since the client has better knowledge of the industry, the technology, and the competitive landscape; a greater ability to anticipate how the stolen information might be used; and possibly greater investigative resources and motivation.

A professional standard requiring disclosure would also align security practices at each law firm with the security expectations of the firm's clients. No attorney wants to call a security-conscious client and tell them their data has been stolen, and that possibility will moti-

---

89. VERIZON ET AL., 2012 DATA BREACH INVESTIGATIONS REPORT 3, *available at* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.

90. *See, e.g.*, BRENNER, *supra* note 7, at 239–44; *How to Protect Your Computer*, FBI, http://www.fbi.gov/scams-safety/computer_protect (last visited May 9, 2013); *Understanding Security and Safer Computing*, MICROSOFT, http://windows.microsoft.com/en-US/windows7/Understanding-security-and-safer-computing (last visited May 9, 2013); *Tips*, U.S. COMPUTER EMERGENCY READINESS TEAM, http://www.us-cert.gov/cas/tips (last visited May 9, 2013).

vate and encourage good security practices by aligning the financial and professional interests of law firms with the needs of their clients. Getting law firm attorneys and staff motivated to employ better secure practices is essential; IT security professionals report that the lack of security awareness among managers and staff is the single biggest obstacle to good information security.[91] Data security should not be an esoteric and mysterious exercise conducted by the IT department, but rather a routine, enterprise-wide component of maintaining strong, productive, and profitable client relationships.

A critic might object that professional standards provide no guarantee of real-world compliance by attorneys.[92] Such objections may seem especially potent in this case, since it is so difficult for the client to detect unreported breaches.[93] However, many of the common professional standards have this quality. Legal clients often cannot tell, for example, whether an attorney is keeping client fees in a separate account until the fees have been earned,[94] is properly supervising office staff,[95] or is billing only those hours actually worked.[96] Nevertheless, the legal profession has established these expectations and many others. When violations come to light, bar investigators and courts enforce those standards using the traditional trifecta of disciplinary measures.[97] Many law firms — especially the larger ones — institute support structures and internal controls to ensure that they meet applicable professional standards,[98] further increasing the impact of professional standards on actual practice habits.

---

91. Bill Goodwin, *Companies Are at Risk from Staff Ignorance*, COMPUTER WEEKLY 14 (Feb. 2004), *available at* http://www.computerweekly.com/feature/Companies-are-at-risk-from-staff-ignorance.

92. Some academics question the effectiveness of professional responsibility standards in modifying the behavior of lawyers. *See, e.g.*, Elliot L. Bien, *Toward a Community of Professionalism*, 3 J. APP. PRAC. & PROCESS 475, 476 (2001); Leslie C. Levin, *The Emperor's Clothes and Other Tales About the Standards for Imposing Lawyer Discipline Sanctions*, 48 AM. U. L. REV. 1, 5–6 (1998).

93. *See supra* Part II.A and Part IV.B.

94. MODEL RULES OF PROF'L CONDUCT R. 1.15(c) (2004).

95. MODEL RULES OF PROF'L CONDUCT R. 5.3(b) (2004).

96. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 93-379 (1993) (discussing billing for professional fees, disbursements and other expenses).

97. This trifecta consists of reprimands, suspensions, and disbarments. *See, e.g.*, *Attorney Discipline*, NEW JERSEY COURTS, http://www.judiciary.state.nj.us/oae/atty_disc/atty_disc.htm (last visited May 9, 2013); *Ethics and Discipline*, MISSOURI COURTS, http://www.courts.mo.gov/page.jsp?id=604 (last visited May 9, 2013); *Lawyer Ethics and Discipline*, OHIO STATE BAR ASSOCIATION (Jan. 10, 2012), https://www.ohiobar.org/ForPublic/Resources/LawFactsPamphlets/Pages/LawFactsPamphlet-9.aspx (last visited May 9, 2013); *Overview*, MARYLAND ATTORNEY GRIEVANCE COMMISSION, http://www.courts.state.md.us/attygrievance/overview.html (last visited May 9, 2013).

98. Geoffrey C. Hazard, Jr. & Ted Schneyer, *Regulatory Controls on Large Law Firms: A Comparative Perspective*, 44 ARIZ. L. REV. 593, 601 (2002).

E. System of Accreditation or Certification for Information Security

One promising avenue for longer-term consideration would be a system of accreditation or certification aimed at information security practices.

A classic problem in the data security field is that most consumers lack the knowledge to tell the difference between good security and bad security.[99] Even customers who are concerned about security rarely have the skills necessary to test a service provider's security. When consumers cannot tell the difference between good products and bad products, free market mechanisms tend to break down.[100] Good security, like many other high-quality products, requires more effort to produce. If the customers cannot tell the difference, firms employing better security are at a competitive disadvantage compared to those who use cheaper, easier, and less-effective methods,[101] resulting in a race to the bottom.

A system of accreditation or certification, if it accurately reflected the defensive strength of a law firm's information security practices, could correct this problem. The client could decide how much security they need and are willing to pay for, and would select a firm (or a level of services within a firm) that matched those needs. A divorce client might not care about data security at all, while a defense contractor would presumably demand the highest possible level of security accreditation. Firms could charge more for the increased security, thus allowing the market to provide the levels of security that customers desire while avoiding the race to the bottom.

Some efforts have already been made in this area. There is an International Organization for Standardization ("ISO") standard for information technology security techniques[102] and "a handful of [law] firms" have earned this certification and "are now using [it] as a selling point to clients."[103] A broader system of certification and active testing is beyond the normal scope of ISO standards, however, and it is unclear who might be capable and willing to administer such a system. It also seems possible that much of the benefit of such a system could be captured just by aligning the interests of the data custodian (in this case, the law firm) with those of the data owner (the client).[104]

---

99. J. Alex Halderman, *To Strengthen Security, Change Developers' Incentives*, IEEE SECURITY AND PRIVACY, Mar./Apr. 2010, at 79, 79.

100. George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q. J. ECON. 488, 500 (1970).

101. Soghoian, *supra* note 20, at 381–82.

102. ISO/IEC 27001:2005.

103. Riley & Pearson, *supra* note 14.

104. *See supra* Part II.B.

V. CONCLUSION

Cybersecurity at law firms could be substantially improved by strengthening two professional responsibility standards.

First, professional responsibility standards should set the "floor" level of acceptable data protection. All practicing attorneys hold secrets in trust for their clients, and have a professional responsibility to protect those secrets in a reasonable manner. In the modern world, data security is an essential component of that responsibility. All attorneys should be expected to take modest steps towards maintaining a minimal level of competent online security: functioning firewalls and virus scanners, regular software updates and patches, reasonable policies on password strength and software downloads, and employee training against deception attacks. The New Jersey rule[105] and the recent changes to the ABA model rules[106] are a good start; other states should expeditiously adopt these or similar rules.

Second, professional responsibility standards should require disclosure to the client when confidential data is lost or stolen. The client has a compelling interest in knowing when confidential data has been stolen and, if timely informed of the breach, may be able to mitigate the damage. Such a standard would encourage better security practices throughout the legal industry, and would also align the attorneys' interests more firmly with those of the clients, encouraging security practices that reflect each client's needs and expectations.

These two measures, combined, would help to plug a substantial hole in security standards at law firms. Reducing hacking and espionage incidents would benefit clients, attorneys, and American industry as a whole.

105. N.J. Advisory Comm. on Prof'l Ethics, Formal Op. 701 (2006).
106. MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (2012).