PREVENTING DATA BREACHES AT LAW FIRMS: ADAPTING PROACTIVE, MANAGEMENT-BASED REGULATION TO LAW-FIRM TECHNOLOGY

Annie Simkus*

Today, law firms of every size are relying on technology more than ever before. However, a firm's investment in securing its information systems pales in comparison to that of its corporate counterparts, leaving law-firm clients' data unnecessarily at risk. Although there has been a modest increase in regulation for firm management overall, law firms have largely ignored the threat of data breaches, failing to adhere to widely accepted information security standards. This lack of compliance has caused cyber criminals to shift their sights from the client to the vulnerable information security systems of law firms. This Note proposes a proactive, regulatory approach to establish a technology infrastructure in law firms, thus ensuring the protection of client information.

TABLE OF CONTENTS

INTRODUCTION 1112

I. REGULATING LAW PRACTICE GENERALLY 1119
A. Professional Self-Regulation as the Model of Choice 1120
B. The Recognition of Broad Ethical Duties of Law-Firm Management Fails to Fill the Gap 1121
C. Rise of Regulation Beyond the Professional Self-Regulation Model 1122

II. ALL THIS "REGULATION" IS INEFFECTIVE FOR CYBERSECURITY IN

---

* J.D., University of Arizona, James E. Rogers College of Law, 2017; M.B.A. Eller College of Management at the University of Arizona, 2017; B.A., Political Communication, The George Washington University, 2009. My deepest thanks to Professors Catherine O'Grady and Ted Schneyer for their thoughtful feedback and detailed comments throughout the writing of this Note. Special thanks to the entire *Arizona Law Review* team for your hard work and expertise. Finally, I would like to thank my father, Michael Simkus, for never hesitating to get on a plane to support me no matter where I was in the world, and to Jason, for your unending encouragement and especially your patience throughout this process.

LAW FIRMS 1123
A. The Mainstream Bar's Approach to Technology Regulation 1123
1. Mainstream Bar Places Burden of Technology on Individual Attorney 1124
2. But Law Firms are the Information Security Decision-Makers 1125
B. The Limitations of Civil Liability as a Preventative Measure for Data Breaches 1127
1. The Standing and Damages Challenges in Data Breach Litigation.....1128
C. Why Current Statutes to Mandate Information Security Are Not a Solution 1129
1. Federal Laws are Too Narrow to Affect All Law Firms 1130
2. With Few Exceptions, State Data-Breach Laws are Purely Reactive ...1132

III. IMPLEMENTING A PMBR SYSTEM TO INCENTIVIZE PROTECTION 1133
A. The Proactive, Management-Based Regulation System to Affect Law-Firm Behavior 1133
B. Using Proactive, Management-Based Regulation for Technology Compliance 1134

CONCLUSION 1137

INTRODUCTION

> "There are risks and costs to a program of action—but they are far less than the long range cost of comfortable inaction."[1]

In early January 2016, Oleras, a Ukrainian broker, posted on a cyber-criminal forum aiming to recruit black-hat hackers to "break" into law firms that specialized in mergers and acquisitions ("M&A").[2] He offered to pay $100,000 and 45,000 rubles and then split equally any insider-trading profits after the initial $1,000,000.[3] Using a sophisticated phishing[4] attack, Oleras's plan was to send

---

1. John F. Kennedy, *The John F. Kennedy University Story*, JOHN F. KENNEDY UNIV., http://www.jfku.edu/About-Us/The-JFK-University-Story.html (last visited Sept. 17, 2017).

2. Claire Bushey, *Russian Cyber Criminal Targets Elite Chicago Law Firms*, CRAIN'S CHI. BUS. (Mar. 29, 2016), http://www.chicagobusiness.com/article/20160329/NEWS04/160329840/russian-cyber-criminal-targets-elite-chicago-law-firms. The list included 46 of the country's largest law firms as well as two members of the UK's Magic Circle. *Id.*

3. *Id.*

4. Phishing relies on social-engineering tactics to deceive individuals into disclosing sensitive personal information through computer-based means. PETER MELL ET AL., NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T OF COMMERCE, SPECIAL PUB. 800–83, GUIDE TO MALWARE INCIDENT PREVENTION AND HANDLING 2–9 (2005), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-83.pdf. More accurately, this specific phishing attack is considered "spear-phishing" because the hacker used relevant context to make the potential users believe they were interacting with a legitimate source. RAMASWAMY CHANDRAMOULI ET AL., NAT'L INST. OF STANDARDS AND

seemingly legitimate emails to lawyers from prominent firms, requesting to profile the lawyers for their M&A work.[5] The hacker would then use the profile information to infiltrate the firms' networks to review corporate information, such as merger documents, letters of intent, and share purchase agreements, with the ultimate goal of executing trades through front companies in Belize and Cypriot bank accounts.[6]

Similarly, in February 2015, the California law firm Ziprick & Cramer, LLP informed its clients that the "Cryptolocker" virus, a type of ransomware, had infected its in-house server by way of an attorney's work computer.[7] According to the Department of Justice, the same virus had already attacked 234,000 computers and collected more than $27 million in ransom fees during the first two months after the virus appeared.[8] Unlike spear-phishing attacks like Oleras's targeted insider-trading scheme, ransomware thieves send out a mass of phishing emails with corrupted links to cast a large net. When an unsuspecting employee clicks the link, malicious software is downloaded onto the user's computer.[9] Generally, the ransom demand is less than $1,000, and companies nearly always pay to avoid any interruption in service.[10] One cybercriminal, for example, targeted a partner at a Kansas law firm, encrypted all of the partner's laptop files, including his Microsoft Excel and Word programs, and demanded $750 within 48 hours.[11]

Of the top 100 firms by revenue, 80% have had at least one data breach, so firms must be prepared to protect themselves from both intentional hacks by malicious actors and unintentional breaches caused by a careless employee or

---

TECH., U.S. DEP'T OF COMMERCE, SPECIAL PUB. 800–177, TRUSTWORTHY EMAIL 18 (2016), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177.pdf.

5. Sharon Nelson, *Russian Cybercriminal Aims to Breach Top U.S. Law Firms*, SENSEI BLOG (Apr. 4, 2016), http://ridethelightning.senseient.com/2016/04/russian-cybercriminal-aims-to-breach-top-us-law-firms.html. The email appeared to originate from an assistant from Business World (a trade journal). *Id.*

6. Bushey, *supra* note 2.

7. Y. Peter Kang, *'Cryptolocker' Virus Holding Law Firm Data for Ransom*, LAW360 (Mar. 9, 2015), http://www.law360.com/articles/629305/cryptolocker-virus-holding-law-firm-data-for-ransom. A ransomware virus encrypts the files on the victim's computer and prevents the user from accessing the files until a ransom is paid. *Id.* In this instance, the firm did not pay the ransom because this virus merely encrypted the files, so they were unreadable. *Id.* The firm asserted that the cyber criminals were not able to read any of the encrypted files, but offered one year of free credit monitoring as a precaution. *Id.*

8. *Id.*; Andres Hernandez, *Law Firm Cyber-Attacks*, ARIZ. ATT'Y, Oct. 2016, at 17, 19.

9. Kang, *supra* note 7.

10. *Id.*; Nicholas Elliott, *Ransomware Is Booming and Companies Are Paying Up*, WALL STREET J.: RISK & COMPLIANCE J. (Oct. 27, 2016), http://blogs.wsj.com/riskandcompliance/2016/10/27/ransomware-is-booming-and-companies-are-paying-up/.

11. Larry N. Zimmerman, *I Was a Victim of Ransomware*, J. KAN. B. ASS'N, Apr. 2016, at 16. In this instance, Larry Zimmerman did not pay the ransom because he had been practicing safe computing standards such as storing the confidential files on removable media. *Id.*

third-party vendor.[12] Compromised data can also be extracted from stolen computers, mobile devices, and other pieces of hardware.[13] For example, in May 2016, an individual physically broke into a law firm and stole a hard drive that contained the Personally Identifiable Information ("PII")[14] of employees at a label-solutions firm, proving that not all cyber breaches happen online.[15] Accordingly, the question is not whether a firm will have a security breach, but when.[16]

Both large and small firms are attractive targets for data theft because clients entrust valuable information to attorneys.[17] Law-firm records contain a variety of sensitive information such as PII, Protected Health Information ("PHI"),[18] Payment Cardholder Information ("PCI"),[19] and even cyber-based

---

12. Susan Hansen, *Cyber Attacks Upend Attorney-Client Privilege*, BLOOMBERG (Mar. 19, 2015), http://www.bloomberg.com/news/articles/2015-03-19/cyber-attacks-force-law-firms-to-improve-data-security.

13. *See, e.g.*, IDENTITY THEFT RESOURCE CTR., DATA BREACH REPORTS 75 (Dec. 29, 2015), http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf. There, an attorney's personal laptop was stolen while he was riding on a San Diego trolley. The firm Atkinson, Andelson, Loya, Ruud & Romo reported the theft to the California Attorney General's Office and offered its clients identity-theft protection services upon notification. *Id.*; *see also* Kim Quarles, *Cyber & Ethical Issues for Law Firms*, WILLISTOWERSWATSON 1, 14 (2016) (notes on file with author).

14. The National Institute of Standards and Technology ("NIST") provides a uniform standard for federal computer systems and defines PII as "information that can be used to distinguish an individual, to trace to an individual, or to link information from separate sources to identify that individual's activities. Examples . . . include name, social security number, date of birth, and biometric data." TIM GRANCE ET AL., NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T OF COMMERCE, SPECIAL PUB. 800-122, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) 2-1 to 2-2 (2010).

15. Robert Abel, *Multi-Color Employee Data Compromised*, SC MEDIA US: THE DATA BREACH BLOG (June 17, 2016), https://www.scmagazine.com/multi-color-employee-data-compromised/article/529689/; Robert Pleasant, *A Stolen Computer Puts Multi-Color Employees at Risk*, SILICONANGLE (June 17, 2016), http://siliconangle.com/blog/2016/06/17/a-stolen-computer-puts-multi-color-employees-at-risk/.

16. Editorial, *Barbarians at the Digital Gate*, WALL STREET J. (Feb. 5, 2013), http://www.wsj.com/articles/SB10001424127887323701904578275920521747756. "[A] U.S. lawmaker with knowledge of intelligence affairs explained that, when it comes to cyber-espionage, there are only two kinds of American companies these days: Those that have been hacked, and those that don't know they've been hacked." *Id.*

17. Carrie A. Goldberg, *Rebooting the Small Law Practice: A Call for Increased Cybersecurity in the Age of Hacks and Digital Attacks*, 38 AM. J. TRIAL ADVOC. 519, 521–23 (2015).

18. PHI is healthcare-based treatment information such as the medical history or health insurance of a client or opponent. EILEEN R. GARCZYNSKI, AM. BAR ASS'N STANDING COMM. ON LAWYERS' PROF. LIABILITY, PROTECTING AGAINST CYBER THREATS: A LAWYER'S GUIDE TO CHOOSING A CYBER-LIABILITY POLICY 6 (2016).

19. PCI means credit/debit card data, including account numbers, expiration dates, and security codes, along with insurance account information. *Id.*

data.[20] The confidential nature of lawyer–client relationships means law firms face threats from multiple players ranging from profit-seeking, entrepreneurial criminals[21] and state-sponsored actors[22] looking to influence deals, to even so-called hacktivists[23] wanting to right a social injustice. Cyber criminals are collaborating to find new methods to unearth troves of information while the legal profession struggles to keep up with this threat.[24]

Clients presumably continue to trust their attorneys and law firms to protect their information because of the long-standing tradition of attorney–client privilege,[25] yet cyber criminals find it easier to break into the network of a law firm than the network of a client.[26] Currently, the American Bar Association

---

20. Cyber-based data includes web browser history, cookie information, metadata, and IP addresses. *Id.* at 7. A handful of state bars have allowed the use of metadata by third parties as long as no human is privy to the communication. *See Metadata Ethics Opinions Around the U.S.*, ABA: LEGAL TECH. RES. CTR., http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html (last visited Feb. 26, 2017).

21. *Ransomware Attacks Set to Quadruple in 2016*, BEAZLEY BREACH INSIGHTS, Oct. 2016, at 2, https://www.beazley.com/Documents/Insights/201610-ransomware-attacks-set-to-quadruple-in-2016.pdf. According to insurance underwriter Beazley, ransomware attacks were likely to quadruple in 2016 because of the increased availability of ransomware toolkits and the success rate that even unsophisticated attackers are experiencing. *Id.* Beazley handled 43 ransomware breaches in 2015, compared to 52 ransomware breaches in the months of July and August of 2016 alone. *Id.*

22. For example, a Washington firm, Wiley Rein, experienced a state-sponsored attack when the firm represented a solar power panel maker in a trade dispute against China. Hernandez, *supra* note 8, at 18.

23. Meghan Kelly, *Anonymous Defaces Haditha Massacre Lawfirm Website, Releases E-mails*, VENTUREBEAT (Feb. 3, 2012), http://venturebeat.com/2012/02/03/anonymous-haditha-massacre-emails/; Elida Moreno & Enrique Pretel, *Panama Law Firms Say Data Hack was External, Files Complaint*, REUTERS (Apr. 5, 2016), http://www.reuters.com/article/us-panama-tax-fonseca-idUSKCN0X3020.

24. Robert Dethlefs, *How Cyber Attacks Became More Profitable than the Drug Trade*, FORTUNE (May 1, 2015), http://fortune.com/2015/05/01/how-cyber-attacks-became-more-profitable-than-the-drug-trade/.

25. Courts have upheld attorney–client privilege and work-product doctrine in discovery interventions. Genesco, Inc. v. Visa, Inc., 302 F.R.D. 168, 189–94 (M.D. Tenn. 2014); *In re* Target Corp. Customer Data Sec. Breach Litig., No. MDL 142522 (PAM/JJK), 2015 WL 6777384, at *2 (D. Minn. Oct. 23, 2015).

26. Timothy J. Toohey, *Beyond Technophobia: Lawyers' Ethical and Legal Obligations to Monitor Evolving Technology and Security Risks*, RICH. J.L. & TECH., Mar. 20, 2015, at 1, 18; J. Randolph Evans & Shari L. Klevens, *Cybersecurity: You Can't Afford to Ignore It Anymore*, DAILY REPORT: IN PRACTICE (Apr. 25, 2016), https://advance.lexis.com/search?crid=617b7800-3330-424c-9ac386853f60de5a&pdsearchterms=LNSDUID-ALM-DLYRPT-1202755900167&pdbypasscitatordocs=False&pdmfid=1000516&pdisurlapi=true; GARCZYNSKI, *supra* note 18, at 6. Corporate clients are requiring law firms to meet certain minimum requirements for information technology protection services and cyber-insurance policies. Karen Painter Randall & Steven A. Kroll, *Getting Serious about Law Firm Cybersecurity*, N.J. LAW., June 2016, at 55 ("This includes [requiring] law firms [to] complete . . . 20-page questionnaires about their threat detection and network security

("ABA"), through the Model Rules of Professional Conduct ("Model Rules"), recommends no specific information technology ("IT") standards or security requirements. Instead, the Model Rules only require *reasonable* standards.[27] While larger firms are following their corporate counterparts and adopting controls recommended by the National Institute of Standards and Technology ("NIST") framework[28] and the International Organization for Standardization ("ISO") 27001,[29] mid-size and small firms are left with fewer resources to understand and mitigate the potential cybersecurity risk.[30]

While growing media attention has increased public understanding of breaches, law firms have "operated inside a bubble of their own making," falling behind the healthcare industry, financial services industry, and the federal government in data security.[31] The lack of regulation has led firms to implement no more than minimal user-awareness training, leading to weak passwords,[32] lack of encryption usage,[33] and poor security practices.[34] Moreover, law firms are not disposing of data properly and sometimes leave terabytes of outdated documents

---

systems, as well as . . . sending their own security auditors into firms for interviews and inspections.").

27. While flexibility of the language accounts for the dynamism of the technology industry, the lack of precise standards provides an enforcement challenge. Drew Simshaw & Stephen S. Wu, *Ethics and Cybersecurity: Obligations to Protect Client Data*, 2015 AM. BAR ASS'N SECT. LAB. & EMP. L. 12 (2015), http://www.americanbar.org/content/dam/aba/events/labor_law/2015/march/tech/wu_cybersecurity.authcheckdam.pdf.

28. Established by Executive Order 13,636, the NIST Framework provides organizations with a set of industry standards and best practices to help reduce and manage cybersecurity risk. NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 1 (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

29. The ISO 27001 provides a specific standard for organizations "to establish[], implement[], maintain[], and continually improve[]" their information security management systems. INT'L ORG. FOR STANDARDIZATION & INT'L ELECTROTECHNICAL COMM'N, ISO/IEC 27001, INFORMATION TECHNOLOGY—SECURITY TECHNIQUES — INFORMATION SECURITY MANAGEMENT SYSTEMS—REQUIREMENTS 1, (2013), https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

30. Nicholas Gaffney, *Law Firm Data Hack Attack Part I*, LAW PRACTICE TODAY (Apr. 14, 2016), http://www.lawpracticetoday.org/article/law-firm-hack-part-i/.

31. *Id.*

32. Weak, default, or stolen passwords caused 63% of reported data breaches in 2016. VERIZON, 2016 DATA BREACH INVESTIGATIONS REPORT 21 (2016), http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.

33. Stephen J. Rancourt, *Hacking, Theft, and Corporate Negligence: Making the Case for Mandatory Encryption of Personal Information*, 18 TEX. WESLEYAN L. REV. 183, 184–86 (2011).

34. Amanda Ciccatelli, *The Security Vulnerabilities Law Firm Hacks Create for Corporations*, INSIDE COUNSEL (June 1, 2016) http://www.insidecounsel.com/2016/06/01/the-security-vulnerabilities-law-firm-hacks-create.

on their servers.[35] As long as attorneys and firms are relying on modern technology, cybersecurity issues will persist.[36] The comparatively low-budget planning and spending on information security suggests current laws, regulations, and policies have not provided sufficient incentives to promote law-firm awareness of these cyber issues and the need to address them.[37]

The convenience and utility of technology cannot be denied, but the victims of data breaches are left bearing the cost of connection as their PII and corporate information[38] too often falls into the wrong hands. Law firms have been left to choose their own cybersecurity standards.[39] However, as firms move more information to the cloud[40] and cyber criminals become savvier, law firms can no

---

35. *See generally* Tammie Fields, *Lawyer Throws Personal Documents in Dumpster*, WTSP (June 1, 2015), http://www.wtsp.com/news/local/lawyer-throws-personal-documents-in-dumpster/236464737.

36. In early 2017, the ABA expanded its line of insurance policies to include cyber insurance for law firms, indicating its recognition that lawyers and law firms are increasingly relying on electronic data. *ABA Begins Offering Cyber Liability Insurance to Lawyers, Law Firms of all Sizes*, AM. BAR ASS'N (Feb. 28, 2017), http://www.americanbar.org/news/abanews/aba-news-archives/2017/02/aba_begins_offering.html.

37. Based on the ABA's 2016 Legal Technology Survey Report, only 53% of respondents reported they or their firm budgeted for technology compared to 58% of respondents who said their firm budgeted for technology in the previous year. Dave Bilinsky & Laura Calloway, *Budgeting and Planning*, ABA TECHREPORT 2016, at 2 (2016), https://www.americanbar.org/groups/law_practice/publications/techreport/2016/planning_budgeting.html. "[T]he largest single group of respondents (29.5%) indicated that they did not know [how much they spend annually on software to manage their practice], followed by 16.3% who reported between $1,000 and $2,999, 13.7% who reported more than $10,000, and around 12% who reported less than $500." *Id.* Although the 200 top law firms are spending up to $7,000,000, or 1.9% of their gross annual revenues, the trend is deficient compared to similar-sized non-legal companies that are spending 5% to 22% of their total gross revenues. *Compare AMLAW 200 Firms Spending as much as $7M per Year on Information Security*, PR NEWSWIRE (Aug. 27, 2015), https://lac-group.com/wp-content/uploads/2015/08/LAC-Group-CCM-Law-Firm-Cybersecurity-Survey-Press-Release-1.pdf, *with* BARBARA FILKINS, IT SECURITY SPENDING TRENDS, SANS INSTITUTE 5 (2016), https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697.

38. GARCZYNSKI, *supra* note 18. Corporate information involves private-company information such as "intellectual property, business strategy, merger and acquisition documents, blueprints, and contracts." *Id.*

39. Debra Cassens Weiss, *Unsealed Suit Targets Law Firm for Alleged Lax Cybersecurity*, ABA JOURNAL (Dec. 12, 2016), http://www.abajournal.com/news/article/unsealed_suit_targets_law_firm_for_alleged_lax_cybersecurity.

40. Cloud computing allows for convenient network access to computing resources such as stored files through a remote server. The cloud model has five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T OF COMMERCE, SPECIAL PUB. 800-145, THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. State bars have weighed the costs and benefits of cloud computing, and the general consensus has been in favor of the cloud

longer avoid the negative attention that comes with cyber attacks.[41] The purpose of this Note is to advocate for an imposed ethical burden on law firms to better protect electronic client information by proactively preventing data breaches.

Part I begins with an overview of how regulation of the legal profession has developed since the rise of law firms: self-regulation, civil liability, and legislative action. Lawyers have long enjoyed the freedom of self-regulation because of the unique "relationship between the profession and the processes of government and law enforcement."[42] However, state supreme courts aim regulations at individual attorneys, and, for the most part, have not held law firms accountable to the Model Rules.[43] With the significant increase of lawyers practicing in firms, the ABA recognized the need for firm management rules by adopting Model Rules 5.1(a) and 5.3(a), which make a firm's lawyer–managers responsible for ensuring that the firm's lawyers and non-lawyers alike conform to the Model Rules. However, states have declined to enforce these two rules.[44] Meanwhile, as firms with centralized management structures grow, external regulation increases in the form of civil liability and legislation.[45]

Despite the modest growth in regulation, there continues to be too little emphasis on the importance of information security in law firms.[46] Part II discusses the ineffectiveness of the current regulatory system in raising information security standards across the profession. Instead, the individual attorney bears the ethical burden of protecting against data breaches and the data-breach victims must carry the risk of their confidential information being exposed.[47] For example, data-breach suits struggle to survive objections to standing because most courts reject the assertion that the risk of information

---

due to its ease of use and constant accessibility, but as the technology evolves so does the risk. Toohey, *supra* note 26, at 6.

41. Randall & Kroll, *supra* note 26, at 54 ("The legal profession is not immune from the threat of a costly cyber incident.").

42. MODEL RULES OF PROF'L CONDUCT pmbl. (AM. BAR ASS'N 2014) ("The legal profession is largely self-governing.").

43. *See* Symposium, *How Should We Regulate Large Law Firms? Is a Law Firm Disciplinary Rule the Answer?*, 16 GEO. J. LEGAL ETHICS 203, 212 (2002).

44. As this Note will later demonstrate, the unenforceability of these two rules has left a regulatory gap for law firms. Ted Schneyer, *Professional Discipline for Law Firms?*, 77 CORNELL L. REV. 1, 19 (1991). Critics of law-firm discipline point to unenforceability and the unnecessary burden on the disciplinary system. *How Should We Regulate Large Law Firms?*, *supra* note 43, at 211–12.

45. David B. Wilkins, *Who Should Regulate Lawyers?*, 105 HARV. L. REV. 799, 807 (1992). *External regulation* is used to refer to any form of regulation that occurs outside of the judicially supervised professional disciplinary agencies. *Id.* at 814 n.57.

46. Steven T. Taylor, *Recent Law Firm Hacking Underscores the Need for Action*, OF COUNSEL, June 2016, at 2, 22.

47. The Model Rules have adapted to the advent of technology and mobile computing by expanding their scope to include an implied duty to protect against data breaches. Goldberg, *supra* note 17, at 536.

exposure is a cognizable injury.[48] Even if a suit establishes standing, plaintiffs rarely overcome the burden of alleging concrete, compensable damages in relation to the injury.[49]

Congress and state legislatures have imposed laws and created regulatory agencies that mandate a standard of PII protection.[50] Still, the statutes have had little effect on the legal profession because either the laws are tailored to protect a narrow range of information, case law has specifically exempted law firms from applicability, or where the statute allows for a private right of action, claimants are unable to show standing.[51]

Finally, Part III proposes a system of proactive management-based regulation ("PMBR") that imposes an ethical burden on law firms to protect client and employee information. The proposed system lends itself particularly well to combatting technology shortcomings because it calls for a responsible lawyer–manager and a proactive regulatory approach. This proposal shifts the regulatory emphasis away from the reactive disciplinary process in favor of a system that actively promotes compliance, increases IT spending, and expands user-awareness training.[52]

I. REGULATING LAW PRACTICE GENERALLY

State supreme courts in tandem with state bar associations have regulated the legal profession using a Professional Self-Regulation ("PSR") model[53] that relies on compliance with a code of professional responsibility, such as the ABA's

---

48. Thomas Martecchini, *A Day in Court for Data Breach Plaintiffs: Preserving Standing Based on Increased Risk of Identity Theft After* Clapper v. Amnesty International USA, 114 MICH. L. REV. 1471, 1490 (2016); *see also* Dana Post, *Plaintiffs Alleging Only "Future Harm" Following a Data Breach Continue to Face a High Bar*, INT'L ASS'N PRIVACY PROFS. (Jan. 28, 2014), https://iapp.org/news/a/plaintiffs-alleging-only-future-harm-following-a-data-breach-continue-to-fa.

49. In order to survive, the claimant must show evidence of identity theft or, as the First Circuit found, the purchase of credit-monitoring services when the claimant had a reasonable basis to prevent future harm. Anderson v. Hannaford Bros. Co., 659 F.3d 151, 166 (1st Cir. 2011) (holding unauthorized charges on plaintiff's account provided a reasonable basis for purchasing credit-monitoring services and thus were compensable damages); Patricia Cave, *Giving Consumers a Leg to Stand On: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits*, 62 CATH. U. L. REV. 765, 777–79 (2013); Martecchini, *supra* note 48 at 1491–92.

50. *See infra* Section II.C.

51. *See infra* Section II.C.

52. Ted Schneyer, *The Case for Proactive Management-Based Regulation to Improve Professional Self-Regulation for U.S. Lawyers*, 42 HOFSTRA L. REV. 233, 257 (2013).

53. Ted Schneyer, *On Further Reflection: How "Professional Self-Regulation" Should Promote Compliance with Broad Ethical Duties of Law Firm Management*, 53 ARIZ. L. REV. 577, 578 (2011). Schneyer uses the phrase *professional self-regulation* to describe the authority that state supreme courts have to regulate lawyers and the subsequent delegation of administrative functions to the bar or a judicial agency to discipline those lawyers. *Id.*

Model Rules.[54] However, attorneys today are practicing much differently than lawyers did when the courts and the mainstream bar first implemented the PSR system.[55] The changes in law practice and law-firm structure are spurring some external regulation in the form of civil and criminal liability, along with federal and state legislation and administrative agency rules.[56] The control that the once-dominant mainstream bar enjoyed has dwindled, so to ensure continued independence from government interference, the legal profession must consider additional modes of regulation to foster ethical compliance.[57]

A. Professional Self-Regulation as the Model of Choice

The licensing practice and organization of lawyers in early U.S. history led to a system of PSR.[58] Even since the frontier era, the local court licensed the individual attorney who then generally worked alone or shared an office with one other attorney.[59] Because the state licensed the individual, disciplinary enforcement also focused on the individual attorney.[60]

Even as recently as 1969, when the ABA adopted its predecessor to the Model Rules, the law practice and practice structures were different than they are today.[61] The profession has grown from 335,242 licensed lawyers in 1970 to 1,315,561 licensed attorneys today, or, perhaps more relevantly, from a ratio of 1 lawyer for every 520 people to 1 lawyer for every 242 people.[62] Over the same

---

54. The Model Rules provide a model framework for state regulation that the state can choose to adopt. E. Norman Veasey, *"Ethics 2000" Chair's Introduction* to MODEL RULES OF PROF'L CONDUCT (AM. BAR ASS'N 2014).

55. Schneyer, *supra* note 53, at 578 n.2. Schneyer refers to the *mainstream bar* as the American Bar Association with the state and local bar associations, excluding all specialty bar associations. *Id.*

56. *Infra* Sections II.B, II.C.

57. Elizabeth Chambliss & David B. Wilkins, *A New Framework for Law Firm Discipline* 16 GEO. J. LEGAL ETHICS. 335, 341 (2003); *How Should We Regulate Large Law Firms?*, *supra* note 43, at 212 ("To have self-regulatory systems that [do not] address those practice contexts, I think, is a lapse in the profession's own duty.").

58. *How Should We Regulate Large Law Firms?*, *supra* note 43, at 2070. ("[T]he bar admissions process, the bar regulation process, the professional responsibility process . . . focuses on individual responsibility.").

59. 2 ANTON-HERMANN CHROUS, THE RISE OF THE LEGAL PROFESSION IN AMERICA 39 (1965).

60. Disciplinary jurisdiction has been based on licensing, and lawyers are licensed, not firms. Ted Schneyer, *Thoughts on the Compatibility of Recent U.K. and Australian Reforms with U.S. Traditions in Regulating Law Practice*, 2009 PROF. LAW. 13, 36.

61. MODEL RULES OF PROF'L CONDUCT preface (AM. BAR ASS'N 2014). The Canons of Professional Conduct were adopted even earlier than the Model Rules, in 1908. *Id.*

62. Robert C. Clark, *Why So Many Lawyers? Are They Good or Bad?*, 61 FORDHAM L. R. 275, 275 n.1 (1992); NATIONAL LAWYER POPULATION SURVEY 1878–2016, at 1, AM. BAR ASS'N, (2016), http://www.americanbar.org/content/dam/aba/administrative/market_research/total-national-lawyer-population-1878-2016.authcheckdam.pdf; LAWYER DEMOGRAPHICS YEAR 2016, at 1, AM. BAR ASS'N, (2016),

period, the number of solo practitioners has remained relatively flat at around 49%, while the percentage of lawyers working at firms with more than 100 lawyers has risen from 0% to 16%.[63] The practice of law once centered on the solo attorney, but the profession has seen a dramatic rise in large firms.[64] This workplace shift calls for a different approach to ensuring ethical compliance.[65]

B. The Recognition of Broad Ethical Duties of Law-Firm Management Fails to Fill the Gap

The increase in the number of attorneys practicing in large, multi-jurisdictional firms led to the introduction of rules that impose general duties on law-firm management to provide an ethical infrastructure for the firm. Specifically, the ABA's Model Rules 5.1(a) and 5.3(a) impose broad managerial duties on partners and partner-like managers in an apparent effort to fill the regulatory gap of the reactive PSR system.[66] Recognizing the shift, New York and New Jersey extended the obligations of the Model Rules to firms as well as lawyers.[67] However, the disciplinary bodies in these states have only admonished or censured a handful of law firms, with no clear impact on law-firm supervision of attorneys and firm ethical infrastructure.[68]

Professor Ted Schneyer, the forefather of the discussion on professional discipline for law firms, cited three primary reasons why these rules have had little

---

http://www.americanbar.org/content/dam/aba/administrative/market_research/lawyer-demographics-tables-2016.authcheckdam.pdf.

63. LAWYER DEMOGRAPHICS YEAR 2016, *supra* note 62.

64. *Id.*

65. Schneyer, *supra* note 44, at 12. According to Schneyer, "[A system of law-firm discipline] could promote firm practices that reduce the risk not only of discipline but also of civil liability, disqualification, and other non-disciplinary sanctions." *Id.*

66. Rule 5.1(a) states the partner or manager "shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct." MODEL RULES OF PROF'L CONDUCT R. 5.1(a) (AM. BAR ASS'N 2014). Similarly, Rule 5.3(a) controls the supervision of non-lawyers and distinguishes itself from Rule 5.1(a) by requiring the partner or manager to ensure with "reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer." MODEL RULES OF PROF'L CONDUCT R. 5.3(a) (AM. BAR ASS'N 2014).

67. *See* N.Y. CODE OF PROF'L RESP. DR 1-104 (2002); N.J. RULES OF PROF'L CONDUCT R. 5.1(a) (1998); *see also* Julie Rose O'Sullivan, *Professional Discipline for Law Firms? A Response to Professor Schneyer's Proposal*, 16 GEO. J. LEGAL ETHICS 1, 3 (2002); Sarah Diane McShea, *Revisiting Law Firm Discipline—Does It Really Work?*, NY LEGAL ETHICS REPORTER (Feb. 1, 2001), http://www.newyorklegalethics.com/revisiting-law-firm-discipline-does-it-really-work/.

68. McShea, *supra* note 67. In fact, the disciplinary agencies of New Jersey and New York have only disciplined four and one law firms, respectively. Schneyer, *supra* note 52, at 258 n.163. Still, the rules are supposed to promote an ethical infrastructure to prevent individual misconduct rather than create an infrastructure as proof of goodwill demonstrating the firm's commitment to ethical compliance. Chambliss & Wilkins, *supra* note 57, at 337.

effect and are "a disciplinary dead letter."[69] First, what he calls the "diffuseness of responsibility" has led to an inability to properly lay blame on partners who a firm assigns personal responsibility for the ethical infrastructure.[70] Because the two rules rely only on the partners' collective management of the firm, all partners are then equally accountable for implementing and managing the structural controls.[71] Second, disciplinary officials and state supreme courts have hesitated in condemning law-firm conduct due to the practical unenforceability of the vague reasonableness standard.[72] Third, the disciplinary process is set up as a reactive system, meaning complainants file a complaint in response to alleged wrongdoing of the individual attorney.[73] The complainant is unlikely to lay blame with the entirety of the law firm, further discouraging the unenforceability of Rules 5.1(a) and 5.3(a).[74] The inability to utilize these rules effectively left law firms relatively unscathed in the PSR system.[75] Although a tempered response, the ABA recognized the need for oversight responsibility because more lawyers were practicing in firms, but these broad managerial rules have not had the desired effect, leading to the spread of external regulation.[76]

C. Rise of Regulation Beyond the Professional Self-Regulation Model

In addition to the advent of broad ethical duties for law firms, the shift also saw a rise in criminal and civil liability.[77] Legal malpractice has steadily increased since the 1970s.[78] But, similar to the reactive nature of the PSR model, liability arises only after a breach of duty has occurred.[79]

Contrary to the legal profession's desire to self-regulate, the federal and state executive and legislative branches directly regulate lawyers who fall under their jurisdiction.[80] Lawyers have had limited success in thwarting "Washington regulation," arguing strict separation of powers is needed for independence from

---

69. Schneyer, *supra* note 44, at 19. "Indeed, it is difficult to find a law review article or bar debate on the subject that does not begin with Schneyer's article." Chambliss & Wilkins, *supra* note 57, at 336.

70. Schneyer, *supra* note 53, at 592.

71. Chambliss & Wilkins, *supra* note 57, at 339.

72. Schneyer, *supra* note 53, at 595–96. "Consequently, although Rules 5.1(a) and 5.3(a) are negligence based, disciplinary counsel ordinarily look for evidence of knowing or reckless violations in order to counter the predictable defense that they are seeking to hold lawyer–managers *vicariously* responsible for first-order misconduct by others at their firms." *Id.* at 596–97.

73. *Id.* at 603.

74. *Id.*

75. *Id.* at 616; *see also How Should We Regulate Large Law Firms?*, *supra* note 43, at 211.

76. Schneyer, *supra* note 44, at 17–20.

77. Schneyer, *supra* note 53, at 578–79.

78. A. Craig Fleishman, *Legal Malpractice: A Brief History in Time*, COLO. LAW., June 1997, at 157, 157.

79. However, unlike in the PSR system, a successful malpractice claim may result in compensatory and punitive damages. Wilkins, *supra* note 45, at 807.

80. Schneyer, *supra* note 53, at 579.

"government domination."[81] However, some argue "the profession's failure to promulgate ethical standards for firms constitutes a significant breach of its duty of self-regulation. This breach threatens not only the quality of modern private practice, but also the credibility of the entire disciplinary system."[82] And, as Part II will illustrate, in the case of technology and information security standards, external entities will find ways to enforce standards if law firms do not regulate themselves effectively and fail to adequately protect client information.

II. ALL THIS "REGULATION" IS INEFFECTIVE FOR CYBERSECURITY IN LAW FIRMS

The current regulatory system fails to substantially impact information security policies within the profession. First, the Model Rules place a specific burden of technology on the individual attorney, as opposed to imposing it on the entire law firm.[83] However, this is unfair to the attorney in a large firm who has no say on the technology practices of the entire firm.[84] Further, at what point should the firm be accountable to the individual attorney and facilitate the requisite systems training that the firm has implemented? Next, the increase in legal malpractice claims might suggest a remedy, but this is not the case in data-breach litigation.[85] The client's ability to affect law-firm behavior and encourage increased IT spending is minimal due to the difficulty in attaining standing for data-breach litigation and the inability to prove damages. Finally, current legislation imposing information security standards is not enough to affect the legal profession because the protected information is too narrowly defined, law firms enjoy exempted status, or clients cannot utilize a statutory remedy for lack of Article III standing.[86]

A. The Mainstream Bar's Approach to Technology Regulation

The mainstream bar has long relied on the reactive feature of PSR, and this is especially true in its approach to regulating the use of technology. The Model Rules and state bar ethics opinions hold an individual attorney accountable for any misuse of technology that may put client information at risk, but do not impose the same duty on the attorney's law firm.[87] For example, whether and how to use cloud computing are decisions that affect an entire firm, but these decisions only highlight the individual attorney's lack of control.[88]

---

81. MODEL RULES OF PROF'L CONDUCT pmbl. (AM. BAR ASS'N 2014); Schneyer, *supra* note 53, at 603.

82. Chambliss & Wilkins, *supra* note 57, at 344–45.

83. *See infra* Section II.A.1.

84. *See infra* Section II.A.2.

85. *See infra* Section II.B.1.

86. *See infra* Section II.C.

87. Furthermore, some state-bar ethics opinions explicitly require that individual attorneys understand the intricacies of their own IT systems but make no mention of the firm. State Bar of Ariz., Formal Op. 05-04 (2005); *see also* State Bar of Ariz., Formal Op. 09-04 (2009).

88. *See* Toohey, *supra* note 26, at 28–31.

1. The Mainstream Bar Places Burden of Technology on Individual Attorney

In 1997, the ABA saw the need for a comprehensive and critical review of the Model Rules of 1982, in part because of inconsistent state ethics codes and the uncertainty of "the influence that technological developments [would have] on the delivery of legal services."[89] The ABA established the Ethics 2000 Commission to consider the impact of technology and provide clear guidance to the modern law practice.[90] The ABA House of Delegates accepted the Commission's amendments in 2002. While the majority of states have accepted the newest amendments, a handful of states have declined to adopt the 2002 amendments, leaving lawyers to rely on state-bar ethics opinions to guide their technology decisions.[91]

Two relevant rule adjustments arose from the 2002 amendments. First, recognizing the rapid evolution of technology, the ABA introduced a comment to Rule 1.1 requiring lawyers to be informed of "the benefits and risks associated with relevant technology."[92] Some states elaborated on this; for example, an Arizona ethics opinion conceptualized the attorney's duty to understand technology as taking competent and reasonable steps to protect a client's information from theft, inadvertent disclosure, loss, or destruction.[93]

Second, Rule 1.6(c) focuses on confidentiality in the attorney–client relationship.[94] It requires a lawyer "to make *reasonable* efforts to prevent the

---

89. E. Norman Veasey, *"Ethics 2000" Chair's Introduction* to MODEL RULES OF PROF'L CONDUCT (AM. BAR ASS'N 2014).

90. *Id.*

91. *Id.*; *States Making Amendments to the Model Rules of Professional Conduct Dates of Adoption*, AM. BAR ASS'N, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/chrono_list_state_adopting_model_rules.html (last visited Aug. 28, 2016) [hereinafter *States Making Amendments*]. Most of the states have adopted the ABA's latest version with the exception of Alabama, Alaska, California, Georgia, Hawaii, Michigan, Texas, and West Virginia. *States Making Amendments*, *supra*.

92. MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 8 (AM. BAR ASS'N 2014).

93. The opinion recognized the use of outside computer-security experts if the technology was too technical for the attorney's know-how. State Bar of Ariz., Formal Op. 05-04 (2005); *see also* State Bar of Ariz., Formal Op. 09-04 (2009).

> It is also important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field. . . . [T]he lawyer must have, or consult someone with, competence in the field of online computer security.

State Bar of Ariz., Formal Op. 09-04 (2009). For example, a lawyer who protects all files with a Secure Socket Layer ("SSL") server that encrypts and password-protects the files would be considered to have taken "competent and reasonable" steps.

94. *See* Swidler & Berlin v. United States, 524 U.S. 399, 403 (1998) (quoting Upjohn Co. v. United States, 449 U.S. 383, 389 (1981)) ("The attorney client privilege is one of the oldest recognized privileges for confidential communications. . . . The privilege is intended to encourage 'full and frank communication between attorneys and their clients

inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[95] Comment 18 gives some meaning to *reasonable efforts* by suggesting a factor test evaluating the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients.[96]

This cost–benefit analysis departs from the tradition of upholding the attorney–client relationship to the fullest extent all while the individual attorney is still bound to uphold his or her fiduciary obligations.[97] The Model Rules and bar opinions call for reasonable efforts but make no reference to how law firms should use various technologies, leaving the individual attorney with the sole duty to protect the client and the client's property.[98]

2. But Law Firms are the Information Security Decision-Makers

Though the Model Rules center on individual attorney responsibility, they do not focus firm responsibility to ensure the security of client information.[99]

---

and thereby promote broader public interests in the observance of law and the administration of justice.'").

95. MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (AM. BAR ASS'N 2014) (emphasis added).

96. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 18 (AM. BAR ASS'N 2014). The Oregon State Bar recognized the lawyer's limitations and provided an exception when hackers use sophisticated methods to breach that would exceed the attorney's reasonable efforts to maintain confidentiality. Oregon State Bar, Formal Op. 2011-188 n.3 (2011, revised 2015).

97. Gregory J. O'Meara, *Some Silver Linings Have Clouds: Common Law Confidentiality in a Fiduciary Frame, Attorneys, and Cloud Computing*, 48 CREIGHTON L. REV. 793, 831 (2015) ("These comments to the Model Rules suggest that the common law duty to protect client confidences crumbles before considerations as mundane as costs and technical difficulty when considering the 'reasonableness' calculus.").

98. *See* MODEL RULES OF PROF'L CONDUCT *passim* (AM. BAR ASS'N 2014). While the firms could be held explicitly accountable for technology decisions made without direct guidance on what is allowed, the proposed solution, as discussed in Part III, calls for specific standards that firms follow to provide a necessary benchmark across the legal profession, such as encryption standards or specific training modules.

99. While the state bar ethics opinions have encouraged the use of new technologies like cloud computing, favoring convenience over the attorney–client relationship, the opinions are nonbinding and could prove misleading. Toohey, *supra* note 26, at 5. ("Although lawyers may have been comforted by ethical opinions finding the use of e-mail or cloud computing appropriate in the past, they can no longer rely on those opinions given dramatically increased security risk."). *See generally Cloud Ethics Opinions Around the U.S.*, ABA: LEGAL TECH. RESOURCE CTR., http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (last visited Feb. 27, 2017).

Firms, in fact, have no ethical responsibility to protect the client.[100] With more than half of all licensed attorneys in the United States practicing in a firm and thus theoretically sharing the costs of IT systems, firms should have an explicit obligation to their attorneys and clients.[101]

In the event of a data breach, attorneys are ethically held responsible because of their fiduciary relationship with their client even though attorneys are unable to do more to ensure that additional protections are enacted.[102] In other words, an associate in a mid-size or large firm likely has little or no decision-making power to choose the IT system her firm utilizes. Instead, a single managing partner or technology committee selects what is best for the entire firm, forcing the rest of the firm into a "collective acquiescence."[103] In fact, in firms of 500 lawyers or more, 55.2% of the lawyers do not know how their firm spends money on technology,[104] a startling revelation considering the attorneys' ethical responsibilities to "keep abreast of . . . the benefits and risks associated with relevant technology."[105]

Based on a legal technology survey conducted in 2016, the technology-purchasing decision makers of firms with more than nine attorneys are either the managing partner, all partners, or an executive committee.[106] IT consultants recommend that firms utilize standing technology committees to address the firms' IT security needs for greater success.[107] Therefore, committees should be sharing the responsibility of technology.[108]

---

100. *See generally* Schneyer, *supra* note 44, at 39 ("Broadly speaking, only clients or others in privity with a lawyer may bring suit in the absence of intentional wrongdoing.").

101. Schneyer, *supra* note 52, at 252; Schneyer, *supra* note 44, at 11 ("[A] disciplinary regime that targets only individual lawyers in an era of large law firms is no longer sufficient.").

102. *See* Schneyer, *supra* note 44, at 16.

103. *Id.* As further discussed in Part III, each member of the technology committee or the managing partner would be designated as the technology lawyer–manager and thus would be accountable for preventing data breaches and liable for any loss of information.

104. Dave Bilinksy & Laura Calloway, *Budgeting & Planning*, ABA TECHREPORT 2015, at 1, 2 (2015), http://www.americanbar.org/content/dam/aba/publications/techreport/2015/budgeting/Budgeting-Planning.authcheckdam.pdf.

105. MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 8 (AM. BAR ASS'N 2014).

106. In medium firms of 10 to 99 lawyers, 30% of firms use executive committees for their technology decisions compared to 64% of large firms of over 100 lawyers that use executive committees or technology committees. Bilinksy & Calloway, *supra* note 104, at 3.

107. PHILIP M. ZAWA & ALAN S. GUTTERMAN, HILDEBRANDT HANDBOOK L. FIRM MANAGEMENT §13:5, Westlaw (database updated Aug. 2016) (highlighting that diverse membership and the members' commitment to technology is critical to the committee's effectiveness).

108. That is not to say that the individual attorney escapes accountability, especially, when the attorney is individually responsible, say, for losing his personal laptop.

In addition to selecting IT systems and allocating IT funds, the firm, or a representative of the firm, also determines whether to use a third-party service provider, such as an Internet service provider that hosts the law firm's server.[109] As the law firm of McKenna Long & Aldridge learned when a hacker gained unauthorized access to the firm's server at the third-party provider's facility, an offsite server should raise significant data-breach liability concerns for the law firm.[110] In particular, in more than two-thirds of contracts, the third-party vendor will indemnify the law firm up to a certain amount, such as three months of service fees.[111] However, when the median cost of a single data breach is $6.7 million, the standard indemnification provisions are wholly inadequate.[112] Because arranging such contracts is the responsibility of the individuals managing the law firm, holding the individual attorney ethically responsible is inconsistent with practice.

B. The Limitations of Civil Liability as a Preventative Measure for Data Breaches

Holding the individual attorney accountable for a decision he or she did not make or have the power to influence seems unfair to that attorney. However, the larger concern remains with the victims of a data breach. As a matter of malpractice law, if an individual lawyer is liable, then the firm is likely vicariously liable as well.[113] However, in most instances, current law does not afford the victims of law-firm data breaches a remedy because plaintiffs have difficulty proving standing, and even if plaintiffs are able to establish standing, damages are as difficult to assert.[114]

In cases when the entire firm is breached, however, the burden should be shared among the firm and the technology decisionmakers.

109. 2015 LEGAL TECHNOLOGY SURVEY REPORT 20–21, AM. BAR ASS'N (Joshua Poje ed., 2015).

110. *See* Hernandez, *supra* note 8, at 18–19; Allison Grande, *McKenna Long Employees' Data Exposed in Vendor Hack*, LAW360 (Mar. 24, 2014), http://www.law360.com/articles/521289/mckenna-long-employees-data-exposed-in-vendor-hack. The highly publicized breach of Target Corporation during the holiday season of 2013 occurred when cyber criminals stole network credentials through a third-party HVAC company that Target contracted to perform routine maintenance in some of its retail stores. Brian Krebs, *Target Hackers Broke in via HVAC Company*, KREBSONSECURITY (Feb. 5, 2014), https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

111. Liam M.D. Bailey, *Mitigating Moral Hazard in Cyber-Risk Insurance*, 3 J. L. & CYBER WARFARE 1, 5 (2014).

112. 2016 COST OF CYBER CRIME STUDY & THE RISK OF BUSINESS INNOVATION 5, PONEMON INSTITUTE, (2016), https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf. Oftentimes, firms are unaware of the disparity in indemnification provisions until their cyber insurance provider recognizes it. Quarles, *supra* note 13.

113. While the firm may not be accountable under the disciplinary rules, the firm would be vicariously liable in malpractice or breach of fiduciary duty suits. However, asserting harm for a finding of damages in a legal malpractice action would likely have its challenges based on data breach case law in other sectors.

114. For data-breach litigation, victims assert the following: (1) negligence, (2) breach of contracts, (3) implied covenants of good faith and fair dealing, (4) bailment, and

1. The Standing and Damages Challenges in Data-Breach Litigation

Victims of data breaches have brought multiple, yet mostly unsuccessful, claims against companies for exposing the victims' personal and medical information.[115] About 75% of plaintiffs' attorneys allege negligence in data-breach litigation, but plaintiffs have been unable to get to the standard-of-care issue due to difficulties in attaining standing.[116] "A victim of a data breach must principally rely on a theory of increased risk of identity theft in order to recover."[117] Many courts have denied standing, refusing to recognize an increased risk of identity theft as an injury-in-fact.[118]

Moreover, when claims survive an attack on standing, plaintiffs still struggle to prove damages.[119] Some courts have recognized the cost of monthly identity-theft monitoring services as damages. However, negligence actions may not be worth the cost of trial when identity-theft monitoring services range from $25 to $60 per month.[120] While some courts have recently granted Article III

---

(5) conversion; along with common law claims of: (6) unjust enrichment, and (7) restitution. *See generally In re* Ashley Madison Customer Data Sec. Breach Litig., No. 2669, 2016 WL 1366616, at 1 (E.D. Mo. Apr. 6, 2016); Columbia Cas. Co. v. Cottage Health Sys., 2:15-CV-03432, 2015 WL 4497730 (C.D. Cal. July 17, 2015); Genesco, Inc. v. Visa, Inc., 302 F.R.D. 168, 171 (M.D. Tenn. 2014); Dittman v. UPMC, 2015 WL 4945713 at *6, *7 (Penn. Com. Pl. Civil Div. May 28, 2015) ("These entities are victims of the same criminal activity as the plaintiffs. The courts should not, without guidance from the Legislature, create a body of law that does not allow entities that are victims of criminal activity to get on with their businesses.").

115. *See In re* Horizon Healthcare Servs., Inc. Data Breach Litig., No. CIV.A. 13-7418 CCC, 2015 WL 1472483, at *1 (D. N.J. Mar. 31, 2015) (holding plaintiffs did not have standing because there was no economic injury and no imminent risk of harm), *vacated*, 846 F.3d 625 (3d Cir. 2017).

116. John Biglow, *It Stands to Reason: An Argument for Article III Standing Based on the Threat of Future Harm in Data Breach Litigation*, 17 MINN. J.L. SCI. & TECH. 943 (2016).

117. Ariel Emmanuel, *Standing in the Aftermath of a Databreach*, 4 J.L. & CYBER WARFARE 150, 154 (2015). The Seventh Circuit has split from other circuits, leaving an opening for the Supreme Court to resolve this standing issue in the upcoming years. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 697 (7th Cir. 2015) (reversing district court's decision holding that plaintiffs have adequately alleged standing under Article III); Enslin v. The Coca-Cola Co., 136 F. Supp. 3d 654, 680 (E.D. Pa. 2015); Biglow, *supra* note 116, at 955–57.

118. Martecchini, *supra* note 48, at 1491–92; *see, e.g.*, Whalen v. Michael Stores, Inc., 153 F. Supp. 3d 577, 583 (E.D.N.Y. 2015) ("Simply put, Whalen has not asserted any injuries that are 'certainly impending' or based on a 'substantial risk that the harm will occur.'"); Maglio v. Advocate Health & Hosps. Corp., 40 N.E.3d 746, 756 (Ill. App. Ct. 2015) (affirming the trial court's dismissal because of lack of standing due to speculative injury), *appeal denied*, 39 N.E.3d 1003 (Ill. 2015).

119. *See* Post, *supra* note 48.

120. *Identity Theft*, NAT'L ASS'N OF INS. COMMISSIONERS, http://www.naic.org/documents/consumer_alert_idtheft.htm (last visited Oct. 12, 2017). A 2015 Ponemon Institute Study found the average cost per lost or stolen record is $217.

standing, case law has shown that "individuals have no general, freestanding right to have their personal data stored securely."[121] Given the limited availability of remedies, a shift from a reactive to a proactive approach to technology will provide clients more protection before a breach even occurs.[122]

C. Why Current Statutes to Mandate Information Security Are Not a Solution

Federal and state legislatures and administrative agencies have adopted statutes and regulations to promote information security for consumer data in fields such as medical health.[123] Nevertheless, law firms may not yet be required to meet stricter information security standards because the statutes and rules are too narrowly construed, expressly exempt lawyers, or do not enable victims to overcome objections to Article III standing when attempting to pursue private rights of action.[124]

Some of the federal laws governing data breaches include the following: the Computer Fraud and Abuse Act ("CFAA"); the Health Insurance Portability and Accountability Act ("HIPAA") along with the Health Information Technology for Economic and Clinical Health Act ("HITECH"); the Graham–Leach–Bliley Act; and the Red Flags Rules of the Fair and Accurate Credit Transaction Act ("FACTA").[125] Yet, none of these statutes specifically address law firms and lawyers. Comparatively, most states have passed data-breach notification statutes, requiring specific actions in the aftermath of a breach.[126] However, a handful of states have passed statutes that require private companies to develop, implement, and maintain reasonable safeguards to protect sensitive consumer data.[127]

Randall & Kroll, *supra* note 41, at 57. Therefore, if awarded at all, damages would likely be less than $217.

121. Rancourt, *supra* note 33, at 199. *See generally In re* Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482 (D. Minn. 2015) (granting financial institutions class action certification following a showing of standing after computer hackers stole 40 million consumers' credit card and debit card information), *appeal dismissed* (June 23, 2016).

122. *See generally* Post, *supra* note 48.

123. Bailey, *supra* note 111, at 10–11 (2014). PII means Personally Identifiable Information. GRANCE ET AL., *supra* note 14, at 1-1.

124. Rachael M. Peters, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 ARIZ. L. REV. 1171, 1187 (2016). For example, state and federal statutes allow a delay in notifying so as not to interfere with a law enforcement investigation. *Id.* at 1182.

125. *Id.* at 1177. The Electronic Communications Privacy Act ("ECPA") is also a federal privacy law but was intended for protection from government intrusion rather than providing a remedy for a data-breach violation. *Id.* at 1179.

126. *See infra* note 147.

127. Daniel McKellick, *Massachusetts Attorneys in the Cloud—How Massachusetts Regulations and a Classification System Can Provide More Than A Wisp Of Guidance Through The Fog Of Ethical Cloud Computing*, 37 W. NEW ENG. L. REV. 175, 191 (2015); *see also infra* notes 150–51.

1. Federal Laws are Too Narrow to Affect All Law Firms

The federal laws listed above aim to combat cyber threats in various industries in various ways. The CFAA is designed chiefly to criminalize hacking, but it also created a limited right to bring a private civil action for a data breach.[128] That right, however, is triggered only when the victim has suffered at least $5,000 in aggregated damages or the damages affected ten or more protected computers during a one-year period.[129] With the average cost of a stolen record at $217, the $5,000 minimum clearly limits the effectiveness of the CFAA.[130]

HIPAA was designed to protect the privacy of health records, ensure adequate protection standards, and require notification of a breach.[131] With a thief's average payday for stolen PHI at $20,000 per record, compared to $2,000 per record for standard identity theft,[132] medical identity theft is a lucrative business for criminals. Medical identity theft costs the consumer an average of $13,500, and a third of medical identity-theft victims even lost their health insurance to boot.[133] Such a costly problem caught Congress's attention, leading to penalties of $50,000 per violation up to $1.5 million per year.[134]

HITECH expanded the scope of HIPAA for greater dissemination.[135] Specifically, when any data breach affects over 500 individuals, the HIPAA covered entity is required to report the breach to the Secretary of Health and Human Services, prominent media outlets in the state or jurisdiction, and to the Health and Human Services website.[136] Unlike hospitals, law firms are not covered

---

128. 18 U.S.C. § 1030(g) (2012).

129. § 1030(c)(4)(A)(i).

130. *Supra* note 120 and accompanying text.

131. Pub. L. No. 104-191, § 1173, 110 Stat. 1936, 2025–26 (1996) (codified as amended at 42 U.S.C. 1320d–2 (2012)).

132. Jim McKay, *Identify Theft Steals Millions from Government Health Programs*, GOVTECH (Feb. 12, 2008), http://www.govtech.com/security/Identity-Theft-Steals-Millions-from-Government.html. The thief stealing the data can expect a street value of $50 for a stolen medical identification number compared to $1 for a stolen social security number. *Id.*

133. Nick Tate, *Another Health System Hacked: How Safe is Your Medical Info?*, NEWSMAX (Aug. 10, 2016), http://www.newsmax.com/Health/Health-News/medical-identity-theft-id/2016/08/09/id/742866/.

134. 42 U.S.C. § 1320d-5(a)(3)(D). Recently, two health-care organizations paid $4.8 million to settle their own HIPAA charges. *Data Breach Results in $4.8 Million HIPAA Settlements*, U.S. DEP'T OF HEALTH AND HUMAN SERVICES (May 7, 2014), http://www.hhs.gov/about/news/2014/05/07/data-breach-results-48-million-hipaa-settlements.html [http://wayback.archive-it.org/3926/20170127095422/https://www.hhs.gov/about/news/2014/05/07/data-breach-results-48-million-hipaa-settlements.html].

135. Pub. L. No. 111-5, §§13001-424, 123 Stat. 115, 226–279 (2009); Megan Bradshaw & Benjamin K. Hoover, *Not so Hip?: The Expanded Burdens on and Consequences to Law Firms as Business Associates under HITECH Modifications to HIPAA*, 13 RICH. J.L. & PUB. INT. 313, 323 (2010); Randall & Kroll, *supra* note 41, at 55–56.

136. § 13402(e)(3), 123 Stat. at 261–62 (2009) (codified as amended at 42 U.S.C. § 17932 (2012)).

entities, but an attorney who receives PHI is considered a Business Associate and must follow HIPAA guidelines.[137] Law firms that represent a hospital or other health-care entity fall under HITECH, a fact of which lawyers and firms are largely unaware.[138] Together, HIPAA and HITECH have the potential to encourage law-firm compliance with strict requirements and heavy fines for noncompliance. But, of course, most firms fall outside the ambit of these two acts.

Like HIPAA and HITECH for medical entities, the Gramm–Leach–Bliley Act requires financial institutions to disclose their privacy policies to customers and maintain a comprehensive information security program.[139] Under the Act, financial institutions include entities that process nonpublic personal financial information.[140] By extension, this could include at least some law firms, but the organized bar contested the statute's applicability to law firms and won.[141]

Finally, FACTA requires financial institutions[142] to take measures to prevent identity theft, including security programs and truncation of the last five digits of a consumer's account number.[143] Nonetheless, FACTA makes no reference to data stored electronically and expressly protects only financial information as opposed to all PII.[144] Once again, the law's narrow coverage cannot promote the legal profession's responsible use of technology.[145] Similar to CFAA, FACTA does allow for a civil right of action, and failure to comply with FACTA willfully or negligently may lead to civil liability for up to $1,000 in actual

---

137. Bradshaw & Hoover, *supra* note 135, at 322.

138. *See id.* at 333.

139. Pub. L. No. 106-102, § 501(b), 113 Stat. 1338, 1436 (1999) (codified as amended at 15 U.S.C. 6801(b) (2012)) ("[E]ach agency or authority . . . shall establish appropriate standards . . . to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any consumer.").

140. § 509(3), 113 Stat. at 1443 (codified as amended at 15 U.S.C. § 6809(3) (2012)).

141. N.Y. State Bar Ass'n v. F.T.C., 276 F. Supp. 2d 110, 146 (D.D.C. 2003) (holding attorneys engaged in the practice of law are not subject to the privacy provisions of Graham–Leach–Bliley Act).

142. While a financial institution is traditionally a bank or a savings and loan association, the definition also includes "any other person that, directly or indirectly, holds a transaction account belonging to a consumer." 15 U.S.C. § 1681a(t) (2012). Further:

> [a] transaction account means a deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third persons or others. Such term includes demand deposits, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

12 U.S.C. § 461(b)(1)(C) (2012).

143. 15 U.S.C. § 1681c(g)(1) (2012).

144. Rancourt, *supra* note 33, at 203.

145. Other laws, such as the CFAA, have sharper teeth with the possibility of fines and imprisonment but expressly pertain only to federal computer systems and databases. *Id.* at 203–04.

damages, as well as an award of attorney's fees and punitive damages.[146] But just as with CFAA, plaintiffs are unable to show standing in FACTA cases.

The application of Gramm–Leach–Bliley and HIPAA is so narrow so as to exempt law firms altogether or impose liability only on a small segment of the bar. And although CFAA and FACTA recognize a private right of action, case law has proven the difficulty of attaining standing and showing actual damages.

2. With Few Exceptions, State Data-Breach Laws are Purely Reactive

All but two states have enacted security-breach notification legislation, but the data-breach notification statutes only require the covered entities to notify victims; they do not sanction the individual or organization for lax information security systems.[147] Comparatively, Massachusetts has some of the most extensive proactive information security requirements.[148] If an organization stores, processes, or maintains the personal information of a Massachusetts resident, the organization has an affirmative duty to protect the client's personal information.[149] The Massachusetts statute has the regulatory teeth needed to encourage technology compliance. However, few states have followed the example of establishing their own requirement for a Written Information Security Program ("WISP").[150] Because law firms are generally able to escape most types of information security regulation on the whole, a new regulatory model dedicated to managing these risks is in order.

---

146. *Id.* at 199; 15 U.S.C. § 1681n(a)(1)–(3) (2012); 15 U.S.C. § 1681o (2012).

147. Rancourt, *supra* note 33, at 200 ("Most states have a data breach law but only require the organization to notify the affected individuals whose personal information was lost or stolen."). Alabama and South Dakota are the only two states that have not enacted a data-breach notification statute. *Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Apr. 12, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. While a uniform data-breach notification law would be useful to establish national definitions, a federal statute has the potential to weaken the strict standards that states—such as Massachusetts—have enacted. Divonne Smoyer & Kimberly Chow, *Q&A with Massachusetts AG Maura Healey*, INT'L ASSOC. OF PRIVACY PROF'LS (Aug. 23, 2016), https://iapp.org/news/a/qa-with-massachusetts-ag-maura-healy/.

148. McKellick, *supra* note 127, at 191 ("[F]ew Massachusetts businesses and attorneys escape these comprehensive data security regulations.").

149. *Id.*; 201 MASS. CODE REGS. 17.03 (2017).

150. States such as Oregon, Rhode Island, California, and Texas have imposed some sort of proactive duty on organizations to safeguard data. MELISSA J. KRASNOW, THOMSONREUTERS, WRITTEN INFORMATION SECURITY PROGRAM 2–3 (2016), https://iapp.org/media/pdf/resource_center/Krasnow_model_WISP.pdf; *Data Security Laws: Private Sector*, NAT'L CONF. OF STATE LEGISLATURES (Jan. 16, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

III. IMPLEMENTING A PMBR SYSTEM TO INCENTIVIZE PROTECTION

The legal profession has relied on self-regulation, civil liability, and legislative action to promote sound ethical practices and protect clients. However, the use of new technology without reasonable safeguards exposes attorneys and their clients to undue risk. Technology is now an integral part of the law and information security management remains a top concern for law firms, yet firms have been mired in inaction.[151] To overcome this regulatory shortfall, the profession itself must adopt a new regulation technique to limit the risks associated with new technology.

A. The Proactive, Management-Based Regulation System to Affect Law-Firm Behavior

After a lifetime of scholarship and research, Professor Schneyer proposed the adoption of the proactive, management-based regulation ("PMBR") system.[152] The system has two primary elements: (1) firm-designated lawyer–managers, and (2) proactive collaboration.[153] In Schneyer's proposed PMBR system, the designated lawyer–manager would be responsible for monitoring their firm's ethical infrastructure and providing occasional periodic assessments to state court-appointed regulators.[154]

The second element of proactive collaboration establishes and enforces policies, procedures, and systems to support ethical behavior.[155] In practice, the regulatory body identifies problem areas and develops a self-assessment form for the firm to evaluate its own compliance.[156] The self-assessment affords the firm an opportunity to learn, evaluate its performance, and improve its internal controls in collaboration with, say, court-appointed regulators.[157] Ideally, the PMBR system promotes the firms' accountability for their structural controls[158] and thereby

---

151. In a 2016 survey, 67% of respondents identified security management as their top concern, followed by user adoption and lack of training at 42%. INT'L LEGAL TECH. ASS'N & INSIDELEGAL, 2016 ILTA/INSIDELEGAL TECHNOLOGY PURCHASING SURVEY 11 (2016), http://insidelegal.typepad.com/files/2016_ILTA_InsideLegal_Technology_Purchasing_Survey.pdf.

152. Schneyer, *supra* note 52, at 235.

153. *Id.* at 236–37.

154. Schneyer, *supra* note 53, at 586 (asserting that designating a specific lawyer–manager to be responsible for his or her firm's ethical infrastructure cures the issue of "diffuseness of responsibility" under Model Rules 5.1(a) and 5.3(a)); *see also infra* Section III.B; Chambliss & Wilkins, *supra* note 57, at 337.

155. *See* Schneyer, *supra* note 52, at 240.

156. *See id.* at 242.

157. *Id.* at 244.

158. Chambliss & Wilkins, *supra* note 57, at 348.

reduces disciplinary complaints.[159] More importantly, this step would ensure the profession's continued freedom to self-regulate.[160]

Adopting a PMBR system would be a measured adjustment and not a "regulatory sea change," as opponents have lamented.[161] In fact, the shift to a more proactive interaction between firms and disciplinary regulators has already begun.[162] For example, mandatory continuing legal education ("MCLE") and programs such as Law Office Management Assistance Programs have been established to provide firms with additional support to encourage their compliance.[163] Moreover, both international and now national jurisdictions have adopted elements of the PMBR system.[164] Illinois is officially the first state to adopt the changes to support a PMBR system, and Colorado's Supreme Court is well on its way to adoption with established working groups drafting the state's standards.[165]

B. Using Proactive, Management-Based Regulation for Technology Compliance

A tailored PMBR system to regulate the cyber practices of the legal profession could propel law practice ahead of other occupations in dealing with the growing threat of cyber hacks.[166] Taking proactive steps to avoid misconduct,

---

159. Schneyer, *supra* note 53, at 586.

160. The central theme to the topic of law-firm discipline has been the profession's freedom and right to self-regulate.

> We subscribe to a broader vision of professional self-regulation—one that demands that the profession offer its own regulatory strategy, rather than shifting the burden to malpractice plaintiffs and other external regulators. Thus, we argue that the case for law firm discipline, and by analogy the case for ethical infrastructure within firms, stems directly from the profession's duty—and privilege—of self-regulation.

Chambliss & Wilkins, *supra* note 57, at 341. More sophisticated clients have already begun requiring proof of adequate technology and security protocols in place before hiring a law firm to represent them. Taylor, *supra* note 46, at 23. While this market solution may work for larger, sophisticated clients, the less-sophisticated client may not have the know-how or bargaining power to request the same assurances from the firm.

161. Schneyer, *supra* note 52, at 237.

162. *Id.* at 261–62.

163. Schneyer, *supra* note 53, at 586–87.

164. *See* Joan C. Rogers, *Illinois Kicks Off Era of Proactive Lawyer Regulation*, BLOOMBERG (Feb. 8, 2017), https://www.bna.com/illinois-kicks-off-n57982083522/.

165. *Illinois Becomes First State to Adopt Proactive Management Based Regulation,* SUPREME COURT OF ILL. (Jan. 25, 2017), http://www.illinoiscourts.gov/Media/PressRel/2017/012417.pdf. Starting in 2018, Illinois lawyers in private practice without malpractice insurance will be required to complete a four-hour interactive, online self-assessment of the daily operations of their firm. *Id.* Colorado is also actively pursuing and developing a PMBR system with assessment tools. *Meeting Minutes*, COLO. SUPREME COURT (Jan. 18, 2017), http://www.coloradosupremecourt.us/PDF/AboutUs/PMBR/PMBP%20Subcommittee%20Minutes%201-18-17.pdf.

166. Outside of federal entities, no nationwide entity regulates the information security practices, which is why many have called for either a national data-breach statute or

rather than merely reacting to misconduct, is likely to decrease the number of security breaches and disciplinary complaints.[167]

First, in the PMBR system, specific lawyer–managers take responsibility for the technology risks in a firm's practice.[168] They would play a major role in their firm's technology decisions as well as in ensuring that a proper technology user-training program was in place rather than leaving lawyers in the firm to their own devices.[169] As a small-scale example, HIPAA requires a covered entity to designate a "privacy official who is responsible for the development and implementation of the policies and procedures of the entity."[170] The designated lawyer–manager would operate in a similar way.[171] The individual would be responsible for compliance by managing user training programs to ensure employees understand the firm's information security policies, as well as verifying firm compliance with standards for electronic storage of client files.

Second, the lawyer–manager would conduct periodic self-assessments focused on technology compliance. Organizations such as financial institutions, government agencies, and insurance companies saw a decrease in data breaches once they implemented regular assessments.[172] While free to create a new set of standards, state regulators should adopt one of the two most widely accepted standards of information security: the NIST Framework or ISO 27001 certification.[173] In some cases, the client may already demand proactive management of the firm's IT systems with their own self-assessment forms.[174]

---

a regulatory agency such as the FTC or SEC to take control and implement controls. Peters, *supra* note 124, at 1201.

167. *See* Schneyer, *supra* note 52, at 246. In New South Wales, studies found an average reduction in complaints by two-thirds after the initial self-assessment. *Id.*

168. *Id.* at 240.

169. *See* Randall & Kroll, *supra* note 41, at 56 ("[L]aw firms must train employees so they are aware of the company's security protocol and are protected against the potential for accidentally exposing a client's personal, confidential information with the click of a button."). In 2015, only 34.1% of firms reported having a dedicated Chief Information Officer or other staff person in charge of the firm's data security. 2015 LEGAL TECHNOLOGY SURVEY REPORT, *supra* note 109, at I-39.

170. 45 C.F.R. § 164.530(a)(1)(i) (2017); Bradshaw & Hoover, *supra* note 135, at 329.

171. For larger firms, the designated lawyer–manager would act in a similar capacity on a larger scale as a Chief Information Security Officer ("CISO"). Evidence has shown that companies with an appointed CISO have decreased their data-breach costs by 4%. 2016 COST OF CYBER CRIME STUDY & THE RISK OF BUSINESS INNOVATION, *supra* note 112, at 9 fig.7.

172. Analysts argue an internal audit can encourage a work culture that recognizes and understands data breaches throughout the entire organization. MARK HARDY, SANS INST., FROM THE TRENCHES: SANS 2016 SURVEY ON SECURITY AND RISK IN THE FINANCIAL SECTOR 6 (2016), https://www.sans.org/reading-room/whitepapers/analyst/trenches-2016-survey-security-risk-financial-sector-37337.

173. *Supra* notes 49 and 50 and accompanying text.

174. The client's assessment forms are likely based off NIST and ISO standards because of SEC or FTC regulation of the corporate client. Extra measures may require

Based on the current cyber threat, users remain the organization's greatest vulnerability.[175] Training is key to creating a workplace culture that understands technology and the threats surrounding it. Currently, survey data indicates 70.5% of lawyers have access to one or more types of training with only 24.5% of that training being live classes offered by in-house staff.[176] The Florida Bar took the deficiency of technology training into its own hands and added three hours to its MCLE requirements focusing purely on technological competence, thus demonstrating the bar's recognition of the undeniable importance of technology in modern law practice and the value of preventing new problems before they arise.[177]

In addition to self-assessment, a cybersecurity PMBR system expands the proactive element to include information sharing. As it is now, law firms are hesitant to publicize data breaches, creating a barrier to access information.[178] By sharing information through a central entity, law firms will be able to identify and share threats to prevent and respond to data attacks. For example, the legal community established an Information Sharing and Analysis Organization[179] dedicated to the legal services, better known as LS-ISAO, in 2015 following the

---

bringing in outside professionals. Taylor, *supra* note 46, at 23. "Law firms need to engage cybersecurity experts to audit their IT systems and reasonably assure them that they've done everything they can to protect data and guard against hacking." *Id.* "The partnerships that hackers may have on their hit lists often are those that work with companies that are, in fact, regulated by a government agency like the SEC or FTC, which monitor how these companies manage their information and ensure that their data is safe from intrusion." *Id.* at 2.

175. Most cyber attacks rely on social-engineering techniques, meaning the attack originates from outside of the organization but requires user action to be harmful, such as clicking on a malicious link or responding to a bogus email. User awareness training has been effective to combat these criminal techniques. HARDY, *supra* note 172, at 9.

176. Mark Rosch, *Technology Training,* ABA TECHREPORT 2016, at 3–4 (2016), https://www.americanbar.org/content/dam/aba/publications/techreport/2016/training/technology-training.authcheckdam.pdf.

177. John Stewart & Casey Flaherty, *Mandatory Tech CLE: An Idea Whose Time Has Come*, LEGAL REBELS (Dec. 1, 2016), http://www.abajournal.com/legalrebels/article/mandatory_tech_cle_an_idea_whose_time_has_come/?utm_source=internal&utm_medium=navigation&utm_campaign=most_read.

178. Toohey, *supra* note 26, at 19. "Few law firm hacks been publicized, most likely because the firms are reluctant publicly to expose their vulnerability and may not legally be required to inform the public of hacks." *Id.* Most recently, the global law firm DLA Piper reportedly instructed its attorneys and staff to not speak to the press as the firm spent days attempting to bring its email and phone servers back online. Jeff John Roberts, *Law Firm DLA Piper Reels Under Cyber Attack, Fate of Files Unclear*, FORTUNE (June 29, 2017), http://fortune.com/2017/06/29/dla-piper-cyber-attack/. The same attack crippled the international shipping company Maersk and drugmaker Merck, sending them back to 1990s technology. *Id.*

179. CYBERSECURITY UNIT, U.S. DEP'T OF JUSTICE, BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS 5–6 (2015), https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf.

issuance of Executive Order 13691.[180] Although relatively small in comparison to its financial-services counterpart, the LS-ISAO has the necessary foundation to be the central information-sharing entity for law firms, especially with state-bar support.[181] By creating a group of technology regulators, law firms via the regulators are more readily able to share information about technology threats.[182] Additionally, the group of technology regulators would be comprised of cybersecurity experts, thus giving all sizes of firms access to specialists when the expense may have otherwise been too costly.[183]

With the frequency of security breaches, cybersecurity professionals argue for a shift from a defensive posture to a more proactive approach to mitigate risks and make breaches manageable.[184] A proactive approach allows the legal profession to adapt to the rapid development of technology and the threats that face it.[185]

CONCLUSION

The advent of technology has ushered in a new era of immediate access and expanded knowledge at the cost of some of the basics of law practice.[186] The PMBR regulatory system lends itself particularly well to combatting technology

---

180. The Executive Order directed the Department of Homeland Security to encourage the development of ISAOs; however, the ISAOs are member-driven and privately funded by the members. *Legal Services Information Sharing & Analysis Organization, LS-ISAO, Launches With the Help of the Financial Services Information Sharing & Analysis Center*, FIN. SERV. INFO. SHARING & ANALYSIS CTR. 1, 1 (Aug. 19, 2015), https://www.fsisac.com/sites/default/files/news/LS-ISAO-FS-ISAC-Press_Release_Aug%2019%20WEB.pdf.

181. As of February 2017, the LS-ISAO reported 113 member firms and is the fastest growing industry ISAO. *LS-ISAO Announces New Threat-Sharing Membership Tier*, FIN. SERV. INFO. SHARING & ANALYSIS CTR. 1, 2 (Feb. 23, 2017), https://www.fsisac.com/sites/default/files/news/LS-ISAO%20Core%20Tier%20news%20release%20FINAL%2023%20Feb%202017.pdf. Sharing communities are "recognized as one of the best defenses against cyber threats and attacks" yielding "actionable intelligence for dissemination in real-time." *Id.* Randall & Kroll, *supra* note 41, at 54. ("[L]aw firms will be able to submit their own information anonymously regarding a cyber incident.").

182. Cybersecurity issues have gone unnoticed for as long as they have partially because the profession does not speak to one another when it comes to breaches.

183. Rancourt, *supra* note 33, at 212–13 ("Forcing every entity in the count[r]y that stores personal information to create a lengthy security programs seems far too costly to implement correctly.").

184. Once an organization recognizes its inability to protect against data breaches at any moment, the organization can adopt a predictive approach of recognizing cyberattacks as opposed to reacting to the crisis after the breach has already occurred. RAJ CHAUDHARY & DAVE MCKNIGHT, INTERNAL AUDIT FOUNDATION, NEXT STEPS: BEYOND RESPONSE TO ANTICIPATION 6 (2016).

185. *See* Schneyer, *supra* note 52, at 260.

186. Gaffney, *supra* note 30 ("This is an interesting time, where we are seeing age-old legal industry norms like attorney-client privilege and cross-practice collaboration collide headlong with irreversible trends like mobile devices, cloud computing and borderless networks.").

shortcomings because the system calls for (1) a responsible lawyer–manager and (2) a proactive regulatory approach. Holding law firms accountable will prompt an increase in firm resources dedicated to information security, from spending more on IT systems to allotting time for user-awareness training. However, most importantly, adopting a PMBR system allows the legal profession to continue to uphold its tradition of attorney–client confidentiality and its commitment to clients in this technology-driven age.