American University Law Review

Volume 62 | Issue 5 Article 5

2013

Hacker's Delight: Law Firm Risk and Liability in the Cyber Age

Michael McNerney

Emilian Papadopoulos

Hacker's Delight: Law Firm Risk and Liability in the Cyber Age

Keywords
America the Virtual: Security, Privacy, and Interoperability in an Interconnected World, Panetta, Leon E., 1938-, Law firms -- Risk management, Computer hackers, Law firms -- Law & legislation, Executive orders, Liability (Law) -- United States, Cyberterrorism -- Prevention, Cyberspace -- Security measures -- Law & legislation

HACKER'S DELIGHT: LAW FIRM RISK AND LIABILITY IN THE CYBER AGE

MICHAEL MCNERNEY* & EMILIAN PAPADOPOULOS**

TABLE OF CONTENTS

* Mike McNerney is senior consultant with Delta Risk LLC, based in Palo Alto, California. Mr. McNerney provides consulting services to government agencies and private sector companies on cybersecurity, market access, and competitive strategy. Prior to this position, Mr. McNerney served as an attorney and cyber policy advisor in the Office of the Secretary of Defense. Mr. McNerney has also held positions in the U.S. State Department and is a veteran officer of the U.S. Air Force. Mr. McNerney graduated from *UC Davis* and holds a Juris Doctorate from *American University, Washington College of Law*.

** Emilian Papadopoulos is chief of staff at Good Harbor Security Risk Management, where he advises corporate executives, investment professionals, and government leaders on managing cyber risk. Previously for Good Harbor, he advised government and commercial clients in the Middle East and North America on strategic security planning in the areas of technology, urban design, transportation, and emergency management. Before joining Good Harbor, Mr. Papadopoulos worked as a communications professional for the Government of Canada in Ottawa and at the Canadian Embassy in Washington, D.C. Mr. Papadopoulos holds a Masters of Public Policy from *Harvard University's Kennedy School of Government* and a B.A. (Honours) from the *University of Toronto*.

INTRODUCTION

In October 2012, former Secretary of Defense Leon Panetta made headlines at a speech in New York when he warned of an impending "cyber Pearl Harbor."[1] He cautioned that the United States' critical infrastructure, such as the electric grid, air traffic control system, and financial networks, are increasingly vulnerable to malicious hackers both at home and abroad.[2] Since then, numerous senior government officials also echoed Panetta's comments,[3] and the Administration issued an executive order on improving the cybersecurity of critical infrastructure.[4] The fact that the Administration would dedicate so much attention to cybersecurity shows how important this issue is to our nation's security.

While the U.S. defense establishment gears up to defend the nation from this nightmare scenario, private industry is already locked in a struggle with what is perhaps a more insidious threat: the persistent theft by cyber means of intellectual property and business secrets. Although this threat

1. Leon Panetta, Sec'y of Def., U.S. Dep't of Def., Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York, NY (Oct. 11, 2012), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

2. *Id.*

3. *See, e.g.*, James R, Clapper, Statement for the Record, World-wide Threat Assessment, Senate Select Committee on Intelligence (Mar. 12, 2013), available at http://www.intelligence.senate.gov/130312/clapper.pdf (listing cybersecurity as the top threat to national security); Tom Donilon, U.S. Nat'l Security Advisor, Remarks by Tom Donilon to the Asia Society, New York, NY (Mar. 11, 2013), available at http://asiasociety.org/new-york/complete-transcript-thomas-donilon-asia-society-new-york (noting that China is waging a campaign of cyber espionage against U.S. companies).

4. Exec. Order No, 13636, 78 Fed. Reg. 11737 (Feb. 19, 2013).

probably will not cause the same level of immediate and catastrophic harm as an attack on critical infrastructure, it does promise to undermine America's long-term competitiveness.[5] At a time when the world economy remains fragile, this loss of competitiveness can negatively impact our ability to be productive and generate wealth and economic progress.[6] While the exact scope of the problem is hard to discern, and indeed some people question whether the threat is as severe as experts say, evidence in reports by government and private organizations continues to mount that the cyberthreat to the economy is significant. Most recently, the Commission on the Theft of American Intellectual Property reported that intellectual property theft against the U.S. is costing the economy more than $300 billion per year, nearly equal to the country's total exports to Asia.[7]

In many respects, America remains the center of global technological innovation. The United States is home to many of the world's best research universities and facilities, which helps fuel our high-tech innovation centers in places like Silicon Valley and Boston.[8] Additionally, a great deal of global financial transactions occur in places like New York and Chicago, and the mid-west appears to be on the cusp of an energy boom.[9] All of this is great news and bodes well for the future of the American economy. Unfortunately, it also provides a tempting target for criminal enterprises and nations who do not possess a robust, indigenous

---

5. *See* OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, 2009–2011, at 9–10 (2011), *available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (describing how foreign attacks against the United States seeking economic information through cyber espionage represent a significant and growing threat to the nation's prosperity and security by stealing data acquired by U.S. companies through research and development).

6. *See id.* (explaining how cyberattacks could undermine the United States' ability to successfully negotiate sensitive business deals with foreign countries, affect project financing for energy projects, and allow foreign entities access to important non-public macro-economic data such as interest rate policies).

7. *See* Paul Eckert, *Panel Urges Tougher U.S. Response to Trade Secret Theft*, REUTERS (May 22, 2013, 7:23 PM), http://www.reuters.com/article/2013/05/22/us-usa-china-theft-idUSBRE94L1BL20130522 (explaining that traditional responses from the US have been inadequate in the face of a growing cyber threat).

8. *See* Heike Mayer, *Bootstrapping High-Tech: Evidence from Three Emerging High Technology Metropolitan Areas*, METRO ECON. SERIES (Metro. Policy Program at Brookings), June 2009, at 1–2, *available at* http://www.brookings.edu/~/media/research/files/reports/2009/6/metro%20hightech%20mayer/06_metro_hightech_mayer.pdf (establishing Silicon Valley and Boston as setting the standards against which emerging high-technology centers measure themselves).

9. *See* ENERGY SEC. LEADERSHIP COUNCIL, THE NEW AMERICAN OIL BOOM: IMPLICATIONS FOR ENERGY SECURITY, at ii–iii (2012), *available at* http://www.ourenergypolicy.org/wp-content/uploads/2012/05/document_ew_01.pdf (describing the oil boom and the resulting energy independence as heralding in a new era of economic stability for the United States).

capacity for innovation. As such, it should come as little surprise that others will attempt to steal the United States' intellectual property as a shortcut to their own prosperity. The growth of the Internet and the resulting interconnectedness of our networked world just make would-be thieves' jobs a lot easier—"Recognizing this problem, the Administration in February 2013 issued its *Strategy on Mitigating the Theft of U.S. Trade Secrets*, though the strategy's impact will be limited without significant regulatory or legislative support."[10].

Much like technology itself, the nature of cyberattacks is constantly evolving. Cyberattackers, or hackers, have focused a lot of attention on the fertile hunting ground that is financial institutions, energy companies, defense firms, and information technology companies.[11] Yet, as awareness increases and cybersecurity improves in these industries, intruders have begun to look elsewhere.

Increasingly, law firms are becoming ground zero for theft of intellectual property and business secrets.[12] Attackers realize that law firms can house significant stores of sensitive information for their clients and that hacking a single firm can provide one stop shopping for a wide range of trade secrets and sensitive transactional data.[13] This new dynamic poses significant challenges for attorneys and law firms as they begin to grapple with the implications for their professional responsibility and for their own brand protection and competitiveness.

This Article seeks to examine this new dynamic and its implications for the legal community. Part I begins with an overview of who is committing these cyberattacks, provides a deeper analysis of why law firms have become targets, and includes discussion of some notable hacks. Part II examines the implications and potential liabilities for law firms in the face of such attacks. Lastly, Part III outlines some of the steps that law firms can take to mitigate the threat and protect both the firms' and their clients' vital information from exploitation.

---

10. *See* EXEC. OFFICE OF THE PRESIDENT, ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS (2013), *available at* http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

11. *See* Panetta, *supra* note 1 (explaining current attacks and the drastic potential consequences of future, more serious, attacks, such as hackers being able to shut down power grids, contaminate water supplies, and disable critical military communication networks).

12. *See* David Mandell & Karla Schaffer, *The New Law Firm Challenge: Confronting the Rise of Cyber Attack sand Preventing Enhanced Liability*, LAW PRAC. TODAY (Mar. 2012), http://www.americanbar.org/content/dam/aba/publications/law_practice_today/the-new-law-firm-challenge-confronting-the-rise-of-cyber-attacks-and-preventing-enhanced-liability.authcheckdam.pdf ("Law firms are increasingly becoming attractive targets to hackers for the valuable client data on their servers.").

13. *See id.* (arguing that a corporation's merger and acquisition secrets, or business deals, can be more readily accessible through hacking the network of the corporation's law firm rather than by hacking the corporation itself).

I. WHO IS COMMITTING THESE ATTACKS AND WHY THEY ARE TARGETING LAW FIRMS

A. There Are a Wide Variety of Hackers with Their Own Skill-Sets and Motivations

Before we explore why law firms are targeted, we need to quickly examine who is doing the targeting. We can divide the actors who engage in theft of intellectual property and other business secrets into three broad categories: (1) nation-states; (2) non-state organizations, including criminal enterprises, terrorists groups, and sophisticated hacker communities; and (3) "lone-wolf" hackers and insiders.[14] While there can certainly be linkages between these groups, they largely have their own distinct identities and motivations.[15] Additionally, technical capabilities vary considerably, typically with nation-states having the most, especially with regard to offensive capabilities, and individuals having the least.[16]

When we think of cyber intrusions at the nation-state level, we tend to think mostly about traditional espionage against foreign governments.[17] While this problem certainly exists, there can also be strong motivation for nation-states to engage in some level of corporate or industrial espionage as well. In these cases, national leaders may have determined that their security depends on high levels of economic growth and are therefore willing to leverage government resources to provide their domestic companies with an advantage by supporting cyberattacks on foreign businesses.[18] Intrusions sponsored or approved by nation-states are among

---

14. Chad Brooks, *Cyberattacks on Small Business Occurring More*, BUS. NEWS DAILY (Dec. 1, 2011, 11:18 AM), http://www.businessnewsdaily.com/1740-cyber-attack-costs.html (quoting Didier Lavion, principal in PwC's forensic services practice).

15. *See* Gregory J. Rattray & Jason Healey, *Non-State Actors and Cyber Conflict*, *in* 1 AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 65, 67 (Kristin M. Lord & Travis Sharp eds., 2011) (describing diverse motivations of non-state actors such as revenge, patriotism, greed, and entertainment).

16. *See id.* (discussing the difficulties that individual hackers face and the trend of hacker groups teaming up with governments to provide the hackers with resources and the governments with plausible deniability).

17. *See* Ellen Nakashima, *U.S. Said To Be Target of Massive Cyber-Espionage Campaign*, WASH. POST (Feb. 10, 2013), http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_print.html (examining a classified government report, The National Intelligence Estimate, finding that nation-state cyber espionage was once viewed as a concern mainly for U.S. intelligence and the military, but is increasingly seen as a direct threat to the nation's economic interests such as businesses and firms that hold trade or merger secrets on their networks).

18. *See* Melanie Hart, *China's Need for Innovative, Market-Based Economic Growth*, CTR. FOR AM. PROGRESS (Oct. 5, 2012), http://www.americanprogress.org/issues/china/news/2012/10/05/40683/chinas-need-for-innovative-market-based-economic-growth (describing weak IP enforcement in China as a form of protectionism when domestic innovation is low).

the best funded, most persistent, and most difficult to thwart.[19]

Non-state organizations are generally the second biggest challenge and can be particularly dangerous for industry because they focus a great deal on economic espionage, financial theft, and disruption.[20] Organized criminal enterprises, sometimes with state connections, are developing significant cyber capabilities and can be quite effective at targeting corporate and financial data.[21] These groups have emerged as a significant challenge to banks, small businesses, and law firms over the past few years.[22] Terrorist groups and hacker communities, on the other hand, have less motivation to conduct espionage and, at this point, tend to be more interested in disruption and propaganda.[23]

The final threat comes from individuals.[24] Typically less sophisticated, this category of threat will nonetheless become more challenging as cyber tools become commoditized and available for purchase on the open market.[25] The greater hazard to private enterprises may come from insiders who have ready access to sensitive information and either misuse or mishandle it.[26]

---

19. *See* David Sanger et al., *Chinese Army Unit Is Seen as Tied To Hacking Against U.S.*, N.Y. TIMES (Feb. 18, 2013), http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html (detailing a study giving strong evidence that the most sophisticated of the Chinese hacking groups, the "Comment Crew" or "Shanghai Group," is linked to the Chinese government).

20. *See* J. Nicholas Hoover, *Cyber Attacks Becoming Top Terror Threat, FBI Says*, INFORMATIONWEEK (Feb. 1, 2012), http://www.informationweek.com/cyber-attacks-becoming-top-terror-threat/232600046 (describing non-state hacker groups such as Anonymous and LulzSec as an increasingly prominent threat next to attacks from China and Russia).

21. *See* Asavin Wattanajantra, *RSA Conference: Cyber Criminals and State-Sponsored Spies Working as One*, SC MAG. (Oct. 11, 2012) http://www.scmagazineuk.com/rsa-conference-cyber-criminals-and-state-sponsored-spies-working-as-one/printarticle/263160/ (emphasizing a worrisome trend of cyber criminals being employed by state-sponsored spies or organizations).

22. *See* Julie Cohn, *Is Your Business Ready for Cyber War?*, NBCNEWS (Feb. 14, 2013, 10:21 AM), http://www.nbcnews.com/id/50809654/ns/business-small_business/ (recommending ways for small businesses, law firms, and banks to protect themselves against the increasing threat of state sponsored cyberattacks).

23. *See* Hoover, *supra* note 20, at 2 (discussing hacker groups', such as Anonymous' and LulzSec's, focus on disrupting website services and creating website defacements rather than conducting espionage).

24. *See* Brooks, *supra* note 14, at 2 (highlighting the wide range of cyber criminals, from nation states to lone-wolf perpetrators).

25. *See* Michael Riley & Ashley Vance, *Cyber Weapons: The New Arms Race*, BLOOMBERG BUSINESSWEEK MAG. (July 20, 2011), http://www.businessweek.com/printer/articles/540-cyber-weapons-the-new-arms-race (discussing the growth of the cyberweapon industry with "cyber-weapon makers flourish[ing]" and "selling to the highest bidder").

26. *See* Press Release, CSO Magazine, Deloitte LLP, Software Eng'g Inst. CERT Program at Carnegie Mellon Univ. & U.S. Secret Serv., Insider Threat Center, 2011 Cybersecurity Watch Survey: Organizations Need More Skilled Cyber Professionals To Stay Secure (Jan. 31, 2011) (on file with the American University Law Review) (viewing insider attacks as most costly to organizations, causing not only monetary damages but

B. Modern Technological Advantages Are Making Law Firms More Vulnerable to Cyberattacks

As technology continues to evolve it offers numerous advantages, particularly in allowing people to be connected constantly. Ideally, greater connectedness means improved efficiency, greater comfort, economic growth, and the freer flow of information. Unfortunately, without robust security measures, it also means easier access to sensitive information for adversaries. For attorneys in particular this provides some new challenges.

Attorneys have great need of, and have benefitted tremendously from, modern technological developments. Global commerce and international travel create the need to stay virtually connected to the home office through a variety of remote and mobile devices. Similarly, client relations require near-constant accessibility to attorneys and online access to important documents that might otherwise stay secured in the office. While great for productivity, these circumstances create opportunities for hackers to enter onto corporate networks by breaking into remote systems or compromising mobile devices.

C. Law Firms' Weaker Security Measures and Accessibility to Sensitive Information Are Causing Them Increasingly To Be Targeted by Hackers Seeking Client's Information

Willie Sutton famously robbed banks "because that's where the money is."[27] Similarly, hackers are focusing on law firms because of the vast troves of sensitive information they house on their networks.[28] In addition, those networks may contain information on a large number of clients, have inadequate protection of that information, be subject to few regulations protecting the information, and be maintained by people who have a limited focus on information protection.[29]

Hackers seeking non-public information to gain an advantage on the stock market may target attorneys at law firms that handle mergers and acquisitions deals.[30] This theft can lead to deals thwarted and millions of dollars lost.[31] Attorneys' networks may house similarly vital information on a large number of clients in a large variety of fields.

---

hurting the organization's reputation, and causing system destruction and loss of confidential information).

27. William Keegan, *Triumph of the Wild West Gave the Banking Cowboys Free Rein*, GUARDIAN (Nov. 27, 2010), http://www.guardian.co.uk/business/2010/nov/28/european-debt-crisis-banking-sector-comment/print.

28. *See* Mandell & Schaffer, *supra* note 12 (highlighting the fact that attorneys tend to gather sensitive information about their clients in a single place on their networks).

29. *See id.* (providing suggestions for implementing better security in their networks).

30. *See id.* (describing incidents where China based hackers broke into law firms' networks to attempt to stop a merger or acquisition or to interfere with a business deal).

31. *See id.*

Law firms are hampered in their ability to protect this important information. Unlike their clients in sectors like defense, financial services, or health, law firms are not yet subject to specific industry-wide cybersecurity standards.[32] Without these industry specific standards, knowing how to grapple with increasing connectedness presents a real challenge to firms and their information technology departments.[33] The absence of specific legal industry standards is unlikely to change soon as a direct result of any recent governmental efforts. Neither recent legislative effort on the Hill nor the National Institute of Standards and Technology's (NIST) Cybersecurity Framework standards process that resulted from the recent Executive Order on critical infrastructure are likely to address clear standards for the legal community, though they will raise awareness and expectations about cybersecurity. Additionally, law firms are more vulnerable than their clients are because those clients are often larger companies with more resources to invest in information security.[34] While many law firms have some level of information security, fewer have robust strategies for identifying, prioritizing, and securing their most valuable information.[35] Such strategies are vitally important in case of a cyberattack.

Finally, the culture of law firms, which often emphasizes attorneys being able to access information and serve clients any time, from anywhere, increases vulnerability by placing a premium on convenient, remote access to the network.[36]

---

32. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 26, 29, and 42 U.S.C.) (regulating private information recorded on health care networks); *see also* J. Nicholas Hoover, *New Defense Budget Aims To Improve Cybersecurity*, INFORMATIONWEEK (Jan. 4, 2013) http://www.informationweek.com/new-defense-budget-aims-to-improve-cyber/240145571 (noting the 2013 defense budget's increased focus on cybersecurity and IT).

33. *See HITRUST Expands Cybersecurity Center with Launch of First Cyber Threat Analysis Service for Healthcare Industry*, HEALTH INFO. TRUST ALLIANCE (July 24, 2012), http://hitrustalliance.net/news/index.php?a=111 (describing a project involving leaders in healthcare, business, technology and information security leaders collaborating to develop a comprehensive cyber threat intelligence system specific to health care); *cf.* LOGIIC CYBER SEC. SYS., LINKING THE OIL AND GAS INDUSTRY TO IMPROVE CYBER SECURITY 1–2 (2006), *available at* http://www.cyber.st.dhs.gov/docs/LOGIICbrochureHighRes.pdf (improving cybersecurity in the oil and gas industry through combining and monitoring information in a controlled system).

34. *See* Mandell & Schaffer, *supra* note 12 (emphasizing that law firms generally spend less on securing their systems than other businesses).

35. *See* Jeffrey Brandt, *When Good Enough—Isn't*, LEGAL IT PROFESSIONALS (Mar. 28, 2012), http://www.legalitprofessionals.com/index.php/col/jeffrey-brandt/columns/4087-when-good-enough-isnt (recognizing that while other industries have enhanced their security, "arrogant" attorneys do not pay attention to security notices, causing law firms to be "viewed as the weakest link").

36. *See* Cohn, *supra* note 22 ("Misguided notions of safety have led many small-business owners to skip [cyber] security measures entirely, which is precisely what primes them as a target.").

For all these reasons, law firms are frequently "softer" targets than their clients, making them attractive to hackers. As an official at the Federal Bureau of Investigation (FBI) recently noted, "[a]s financial institutions in New York City and the world become stronger, a hacker can hit a law firm and it's a much, much easier quarry."[37] Determining the best way for each firm to balance security, accessibility, and privacy will greatly improve the posture of corporate networks and information technology policies.

D. There Have Been Many Recent Instances of Both Attempted and Successful Cyberattacks on Law Firms

The evidence suggests that hackers have settled on law firms as attractive targets for at least a few years.[38] One cybersecurity firm that collects intelligence on foreign attackers and helps companies respond to intrusions reported that over eighty U.S. law firms were attacked in 2011.[39] In addition, despite the fact that many cyberattacks go undisclosed to the public, there have been reports of a few attacks that have clearly emphasized the risk of cyberattacks to law firms.[40] In early 2010, law firm Gipson, Hoffman & Pancione observed that its employees were receiving socially engineered e-mails that, while designed to look like they were coming from colleagues within the company, were actually coming from spoofed e-mail addresses and carried malware that could compromise the company's networks.[41] Such attacks, known as "spear-phishing," are a common method through which hackers gain initial access to a target network.[42] At the time of the attack, Gipson, Hoffman & Pancione was

---

37. 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 (quoting Mary Galligan, head of the cyber division in the New York City office of the U.S. Federal Bureau of Investigation).

38. *See Law Firms Prime Targets of Cyber Attacks*, ABA NOW (Feb. 5, 2012) [hereinafter *Law Firms*], http://www.abanow.org/2012/02/law-firms-prime-targets-of-cyber-attacks/ (discussing a poll of attorneys at an ABA panel where all of the members in attendance responded that they believed that their firms had already been the victim of a cyberattack).

39. *See* Riley & Pearson, *supra* note 37 (examining a comprehensive report by Mandiant, a cybersecurity firm headquartered in Arlington, VA).

40. *See* Ashby Jones, *China and the Law: Did Chinese Hackers Attack LA Law Firm?*, WALL STREET J.L. BLOG (Jan. 14, 2010, 9:36 AM), http://blogs.wsj.com/law/2010/01/14/china-and-the-law-did-chinese-hackers-attack-la-law-firm.

41. Alanna Byrne, *Law Firms Are a Prime Target for Hackers*, INSIDECOUNSEL (June 26, 2012), http://www.insidecounsel.com/2012/06/26/law-firms-are-a-prime-target-for-hackers.

42. *See Spear Phishers: Angling To Steal Your Financial Info*, U.S. FED. BUREAU INVESTIGATION (Apr. 1, 2009), http://www.fbi.gov/news/stories/2009/april/spearphishing_040109 (explaining spear-phishing as the practice of sending doctored e-mails, appearing to be from someone the receiver would normally get e-mail from, targeting select groups of people and offering urgent and legitimate-sounding explanations for why the sender needs

representing Cybersitter, a parental control software maker that was involved in a $2.2 billion software piracy suit against companies involved in making the similar Chinese Green Dam filtering software.[43] The firm reported the incident to the FBI, noting that their network had not been compromised because their employees had been made aware of the risk of such spear-phishing attacks and had known not to open the fake e-mails.[44]

That same year, similar spear-phishing attacks targeted the firms Blake, Cassels & Graydon and Stikeman Eliot.[45] At the time of the attack, both firms were involved in a potential $40 billion acquisition by Australian mining firm BHP Billiton of the Potash Corporation of Saskatchewan.[46] Some public reports indicate that hackers, likely international, successfully gained access to the law firm's computer networks, as well as the networks of the Canadian Finance Ministry and Treasury Board, and were able to collect sensitive information from government networks.[47] Ultimately, the Canadian government blocked the acquisition for unrelated reasons,[48] but the determination of hackers to gain sensitive information by targeting law firms clearly highlights the risks to firms.

Foreign attackers are not the only concern for law firms. In 2011, media reports indicated that law firm Hunton Williams had facilitated relationships between cybersecurity firm HBGary Federal and certain clients seeking to disrupt WikiLeaks.[49] In retaliation, the hacktivist group Anonymous publicized sensitive e-mail communications between HBGary Federal and Hunton Williams.[50] HBGary suffered significant reputational damage.[51] Though Hunton Williams' networks may not have been compromised, the fact that hackers revealed sensitive communications between a law firm and its clients further highlights the risks law firms face.

None of this means that law firms necessarily have poor security. Much

---

the soon-to-be victim's personal data).

43. Jones, *supra* note 39.

44. *Id.*

45. Riley & Pearson, *supra* note 37.

46. *Id.*

47. *See id.* ("Over a few months beginning in September 2010, the [China-based] hackers rifled one secure computer network after the next, eventually hitting seven different law firms . . . . Such stolen data can be worth tens of millions of dollars . . . .").

48. *Id.*

49. Eric Lipton & Charlie Savage, *Hackers Reveal Offers To Spy on Corporate Rivals*, N.Y. TIMES (Feb. 11, 2011), http://www.nytimes.com/2011/02/12/us/politics/12hackers.html.

50. *See id.* (describing the leaked documents as including pitches for unethical ways to undermine clients' adversaries).

51. *See* Mark Anderson, *Cyber Security Firm HBGary Bought by ManTech International*, SACRAMENTO BUS. J. (Feb. 28, 2012, 1:37 PM), http://www.bizjournals.com/sacramento /news/2012/02/28/hb-gary-sacramento-man-tech-cyber-securi.html (announcing the sale of HBGary by ManTech International).

to its credit, the legal community is continually making strides in increasing the level of security at firms.[52] Law firms, acknowledging that their actions could make their clients more vulnerable, are learning to use their relatively limited resources more efficiently in order to protect both themselves and their clients.[53] Still, the risks are great. One Washington, D.C. attorney noted that, "[i]f clients start thinking they can't give private information to their lawyers because it might get out, it's a huge problem for the profession. The whole system will start to fail."[54] Furthermore, as customer awareness of cybersecurity issues increases along with further regulations, law suits, and disclosure of cybersecurity incidents, law firms are likely to feel more pressure and expectations to increase their standards for cybersecurity.[55]

II. LAW FIRMS MAY BE INCREASINGLY LIABLE FOR CLIENT'S DAMAGES RESULTING FROM CYBERATTACKS ON THE FIRM.

A. Liability for Law Firms from Cyberattacks May Stem from Current Information Protection Obligations Under Other Disciplines or Authorities

The problem with terms like "cyberlaw" and "cybersecurity" is that they imply a single discipline. The truth is that both are really a hodge-podge of many related but distinct disciplines. In order to fully understand liability for cybersecurity breaches and its potential ramifications for law firms, it is necessary to explore a mix of telecommunications laws, privacy and health statutes, corporate regulations, and court cases.[56]

The vast majority of states have laws governing data breach notification, which were enacted by legislatures in the face of increasing instances of consumer database breaches.[57] California enacted the first of these statutes

---

52. *See* Mandell & Schaffer, *supra* note 12 (highlighting state legislation that holds attorneys liable for data breaches, as well as guidelines that have been developed by the Securities and Exchange Commission and the Federal Trade Commission to advise firms on cybersecurity).

53. *See Law Firms*, *supra* note 38 (recognizing that law firms are prime targets of cyberattacks and suggesting starting points for law firms to enhance cybersecurity such as being aware of the risk, formulating a plan for if their system has been compromised, and formulating a plan to quickly respond); *see also* Brandt, *supra* note 35 (suggesting that law firms take steps such as creating security policies, investing in user education, and hiring a chief security officer in order to reduce the risk and harm of a cyberattack).

54. Riley & Pearson, *supra* note 37 (quoting Richard Goldberg, a lawyer involved in data security).

55. *See* Mandell & Schaffer, *supra* note 12 (using examples of cyberattacks and developing regulations and legislation to argue that these developments, coupled with successful breaches of law firm networks, may increase liability; thus, attorneys will have a heightened standard of care).

56. *See id.* (analyzing how HIPAA and HITECH expose law firms to liability for breaches of patient information).

57. *See id.* (emphasizing that the District of Columbia and forty-six states have enacted data breach notification statutes that require attorneys to notify the state Attorney General's

in 2002,[58] with many states following suit.[59] In essence, California, like most states, requires those who hold personal information about their customers to notify those customers if they reasonably believe that an unauthorized party has obtained their information.[60]

Although the basic concepts of the various statutes are the same, statutes can vary widely from state to state on issues such as notification to law enforcement, the amount of time allowed before contacting those affected, civil or criminal penalties, and private rights of action, among others.[61] While efforts have been made to create a uniform, nation-wide standard for data breach notification, Congress has yet to pass anything.[62] This means law firms and other businesses that possess private client information on firm networks must be prepared to meet the data breach notification requirements of any jurisdiction in which they do business. For large, international firms, this can also mean compliance with international data breach and privacy laws.[63] The European Union, in particular, takes this issue very seriously and has enacted a series of stringent laws covering data breach.[64]

In addition to general data breach notification requirements, those attorneys working in specialized industries may have other more specific obligations. For example, attorneys working in the health care industry should also be familiar with the privacy and security provisions of the

---

office and affected persons in the event of a breach).

58. GINA STEVENS, DATA SECURITY BREACH NOTIFICATION LAWS 1 (2012).

59. *See Breach of Information*, NAT'L CONF. STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/overview-security-breaches.aspx (last visited June 15, 2013) (discussing a data breach incident where the firm initially had to disclose only to California due to its database breach statute, but later had to disclose to several other states as they developed similar laws).

60. *See* CAL. CIV. CODE § 1798.82(a) (West 2013) ("Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system . . . ."); *see also id.* § 1798.29 (extending the same disclosure duty to government agencies).

61. *Compare id.* § 1798.82 (including an individual's medical information within the definition of personal information), *and* MO. REV. STAT. § 407.1500 (2012) (same), *with* CONN. GEN. STAT. § 36a-701b (2012) (failing to include an individual's medical information within the definition of personal information), *and* FLA. STAT. § 817.5681 (2012) (same).

62. *See* Taylor Armerding, *Demise of Cybersecurity Bill Means Executive Order on the Way*, NETWORKWORLD (Nov. 20, 2012, 8:40 AM), http://www.networkworld.com/news/2012/112012-demise-of-cybersecurity-bill-means-264432.html (articulating the failed efforts of Congress in both August and November of 2012 to enact the Cyber Security Act of 2012).

63. *U.S. and Global Data Protection Laws*, MCAFEE, INC., http://www.mcafee.com/us/regulationns/index.aspx (last visited June 15, 2013).

64. *See* Cornelius Rahn, *EU Data-Privacy Rules To Make Breach Disclosures Mandatory Within 24 Hours*, BLOOMBERG (Jan. 23, 2012), http://www.bloomberg.com/news/2012-01-22/eu-s-reding-says-users-to-be-told-of-data-hacks-within-24-hours.html (reviewing the EU bill on data protection rules providing stricter sanctions, requiring disclosure within twenty-four hours of a breach, and allowing national data-protection authorities to levy fines).

Health Insurance Portability and Accountability Act[65] (HIPAA) and the Health Information Technology for Economic and Clinical Health[66] (HITECH) Act. Among other things, HIPPA and HITECH establish policies and procedures for maintaining the privacy of individually identifiable health information.[67] This includes requirements to establish administrative, physical, and technical safeguards to prevent against the loss of health information.[68] To the extent that attorneys have access to this information, they may also be responsible for protecting it.[69]

In addition to data breach laws, there are also several important federal statutes and regulations that impact data security. Perhaps most importantly is the guidance issued by the Securities and Exchange Commission (SEC) in October 2011.[70] Under SEC guidelines, corporations and attorneys are advised to report material cyber risks and incidents to the SEC.[71] Examples of material issues include significant new expenditures on corporate cybersecurity, loss of intellectual property, or incidents that have adverse impacts on customers or clients or even that cause "reputational damage adversely affecting customer or investor confidence."[72] As a result, some publicly traded companies have reported being hacked in their quarterly reports.[73] If this trend continues, the role that laws firms play in these breaches may begin to be highlighted.

The debate over cybersecurity disclosure promises to continue to evolve for several years, and law firms are sure to have an important role in

---

65. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

66. Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified as amended in scattered sections of 42 U.S.C.).

67. *See, e.g.*, 42 U.S.C. § 1320d-6 (2006 & Supp. IV 2011) (criminalizing wrongful disclosure of such information); *id.* § 300jj-11 (Supp. IV 2011) (creating the office of the National Coordinator for Health Information Technology within the Department of Health and Human Services).

68. *See* Megan Bradshaw & Benjamin 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, 329–30 (2010) (analyzing the new safeguard requirements under HITECH exposing parties to both civil and criminal penalties and how they function with the HIPAA security rule requiring parties to implement security policies and procedures).

69. *See id.* at 330 (applying the penalties of violating the Security Rule to business associates, including attorneys).

70. *CF Disclosure Guidance: Topic No.*, U.S. SEC. & EXCH. COMM'N (Oct. 13, 2011) [hereinafter SEC Disclosure Guidance], http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

71. *See id.* ("[A]s with other operational and financial risks, registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cyber-security risks and cyber incidents.").

72. *Id.*

73. *See* Joseph Menn, *Exclusive: Hacked Companies Still Not Telling Investors*, REUTERS (Feb. 2, 2012), http://www.reuters.com/article/2012/02/02/us-hacking-disclosures-idUSTRE8110YW20120202 (exposing reports from companies, including Google and Intel, admitting to successful breaches originating from China).

shaping that debate, as well as being affected by its outcome. For example, many companies have maintained that the SEC guidance was not mandatory and that the uncertainty surrounding cyber risks and incidents minimizes the obligation to disclose.[74] In fact, in issuing its original cybersecurity guidance, the SEC acknowledged discussion by people in the legal profession about how these issues should be handled, highlighting the role the legal profession plays in shaping disclosure requirements.[75]

This SEC guidance goes hand-in-hand with an increasing focus by the Federal Trade Commission (FTC) to ensure that businesses maintain appropriate data security standards and do not make false claims about their own cybersecurity and the protection of customer information.[76] The FTC filed one such complaint against Lifelock, a company that made false claims about preventing identity theft; in 2010, Lifelock agreed to pay $11 million to the FTC, which was to use the funds to issue refunds to certain customers.[77] This increased agency focus on cybersecurity, both as advisors and as enforcers, shows how seriously the government is taking companies' obligations to protect customers from these attacks. That focus could result in increased liability for many professionals who fail to provide adequate security measures.

Since the Lifelock case, the pace of complaints in this area has increased: between May 2011 and December 2012, the FTC filed thirty-two legal actions relating to customer data security.[78] In one recent case, the FTC filed a complaint against hotel chain Wyndham Worldwide Corporation and three subsidiaries for misrepresenting security measures and for failing to safeguard personal information, resulting in "substantial consumer injury" after records of customer's credit card numbers were compromised in repeated attacks against the company.[79] In filing suit against Wyndham,

---

74. *See* Sam Narisi, *Companies Fail to Disclose Data Breaches to SEC*, IT MANAGER DAILY (Nov. 14, 2012), http://www.itmanagerdaily.com/companies-fail-to-disclose-data-breaches/ (detailing an unreported attack on Coca-Cola, where hackers gained access to Coca-Cola's network for at least a month, stealing e-mail and other documents, that was not disclosed due to confusion over whether the breach was material).

75. *See* SEC Disclosure Guidance, *supra* note 70 ("[T]here has been increased focus by registrants and members of the legal and accounting professions on how these risks and their related impact on the operations of a registrant should be described . . . .").

76. *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICY MAKERS, at vii-viii (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf (providing recommendations for businesses to enhance data security practices).

77. Press Release, FTC, LifeLock Will Pay $12 Million To Settle Charges by the FTC and 35 States That Identity Theft Prevention and Data Security Claims Were False (Mar. 9, 2010), *available at* http://www.ftc.gov/opa/2010/03/lifelock.shtm.

78. Jacqueline Klosek, *5 Key Privacy Questions for Hotel Operators*, HOTELNEWSNOW.COM (Dec. 20, 2012), http://www.hotelnewsnow.com/Articles.aspx/9589/5-key-privacy-questions-for-hotel-operators.

79. Press Release, FTC, FTC Files Complaint Against Wyndham Hotels for Failure To Protect Consumers' Personal Information (June 26, 2012), *available at*

the FTC stated that the case was "part of the FTC's ongoing efforts to make sure that companies live up to the promises they make about privacy and data security."[80] The FTC has made it clear it will pursue actions in the realm of data security across multiple sectors.[81]

Considering the sensitive information entrusted to law firms and the extent to which they have been targeted by hackers in the past, it is possible that law firms could find themselves similarly exposed to liability. As with the SEC guidance, the legal community will play an important role in shaping and litigating cybersecurity standards for other companies; in turn, the clients of law firms are likely to continue to increase their expectations of law firm cybersecurity.

B. ABA Ethics Rules, Particularly Those Regarding Confidentiality, May Impose Increased Responsibilities on Attorneys To Protect Clients' Information from Cyberattacks

The legal profession has increasingly embraced emerging technologies to improve the practice of law and enhance its abilities to serve its clients.[82] However, the rules governing the practice of law, including those regarding professional responsibility, can lag behind the technology.[83] This creates special problems for attorneys today, particularly when it comes to ethics and competence.

American Bar Association (ABA) Model Rule 1.1 requires that an attorney provide competent counsel to his or her client.[84] As a part of maintaining competence, attorneys must also "keep abreast of changes in the law . . . including the benefits and risks associated with relevant

---

http://www.ftc.gov/opa/2012/06/wyndham.shtm.

80. *Id.*

81. *See* Press Release, FTC, FTC Testifies on Data Security (June 15, 2011), *available at* http://www.ftc.gov/opa/2011/06/datasecurity.shtm (testifying that since 2001, the FTC has brought 34 cases against a variety of businesses ranging from a human resources processing company to immigration services); *see also* Heather Egan Sussman et al., *Developments at the Federal Trade Commission*, MONDAQ.COM (Jan. 29, 2013), http://www.mondaq.com/unitedstates/x/218496/Data+Protection+Privacy/Privacy+And+Data+Protection+2012+Year+In+Review (describing an FTC suit against Wyndham Hotel and Resorts, a company in the debt collecting industry, and Frankin's Budget Car Sales, Inc., an auto dealer company).

82. *See* Catherine Dunn, *Employees May Be a Company's Greatest Cybersecurity Vulnerability*, CORP. COUNS. (Feb. 21, 2013), http://www.law.com/corporatecounsel/PubArticleCC.jsp?id=1202588933863&Employees_May_Be_a_Companys_Greatest_Cybersecurity_Vulnerability&slreturn=20130125213313 (highlighting some of the technology attorneys have adopted, such as e-mail, smartphones and other mobile devices, and social media).

83. *See infra* note 92 (demonstrating that the ABA ethics rules explicitly addressed the use of cloud computing only since last year).

84. MODEL RULES OF PROF'L CONDUCT R. 1.1 (2011) ("A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.").

technology."[85] Additionally, ABA Model Rule 1.6 establishes the duty of confidentiality and, along with that, Rule 1.4 mandates that attorneys communicate to their clients if there is a breach of confidentiality.[86] These rules require that attorneys take competent and reasonable measures to safeguard client data regardless of the technology that is being used.[87]

A number of states have also weighed in on cybersecurity and professional responsibility. In California, for example, a state bar opinion from 2010 remarks that "[w]hether an attorney violates his or her duties of confidentiality and competence when using technology to transmit or store confidential client information will depend on the particular technology being used and the circumstances surrounding such use."[88] The state bar opinion further requires attorneys to evaluate the level of security in that technology, the legal ramifications of third-party intercept, the sensitivity of the information, possible client impact, urgency, and client instructions.[89] Several other state bars, including Arizona, New Jersey, Pennsylvania, Florida, and New York, have issued similar opinions.[90] The involvement of state bar rules, on top of the ABA requirements, demonstrates the seriousness of attorneys' attempts to prevent incidents where their actions put their clients at risk.

---

85. *Id.* R. 1.1 cmt. 8.

86. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 (requiring that attorneys safeguard information relating to the representation of a client against unauthorized disclosure of access by third parties); MODEL RULES OF PROF'L CONDUCT R. 1.4 (requiring attorneys to keep clients reasonably informed about the status of their case).

87. *See* David Ries, *Cybersecurity for Lawyers: Understanding Ethical Obligations*, LAW PRAC. TODAY (Mar. 2012), http://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/march12/cyber-security-for-attorneys-understanding-the-ethical-obligations.html (extending the duty to protect client data to all developing technologies, such as cloud and mobile services).

88. *See* State Bar of California Standing Comm. on Prof'l Responsibility & Conduct, Formal Op. 2010-179 (2010).

89. *See id.* (describing the steps an attorney must take before using a particular technology in the course of representing a client).

90. *See, e.g.*, State Bar of Arizona Ethics Op. 05-04 (2005), *available at* http://www.azbar.org/Ethics/EthicsOpinions/ViewEthicsOpinion?id=523 (providing that attorneys must take "competent and reasonable" measures to ensure unauthorized access to client information); New Jersey Bar Ass'n Advisory Comm. on Prof'l Ethics, Op. 701 (2006), *available at* http://njlaw.rutgers.edu/collections/ethics/acpe/acp701_1.html (providing that an attorney exercise "reasonable care" in protecting client information from unauthorized access); New York State Bar Ass'n Comm. on Prof'l Ethics, Op. 842 (2010), *available at* http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&CONTENTID=42697&TEMPLATE=/CM/ContentDisplay.cfm (providing that attorneys must take reasonable care to protect confidential client information and must consider the sensitivity of the information prior to storage or transmittal); Pennsylvania Bar Ass'n Comm. on Legal Ethics & Prof'l Responsibility, Formal Op. 2011-200 (2011), *available at* http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf (providing that attorneys must take reasonable care when using cloud computing to transmit and store information so as to assure all confidential client information remain confidential and reasonable safeguards are used to prevent unauthorized access).

A few states and the ABA have also issued specific opinions regarding the use of cloud computing for attorneys.[91] While use of cloud computing is certainly permissible, attorneys must take into account security and third-party access when using these services. For example, under ABA Model Rule 5.3, cloud-computing providers could be considered to be non-lawyer providers.[92] In order to comply with that rule, an attorney using cloud-based services would have to "make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations."[93] According to Nicole Black, Vice President at MyCase, "[l]awyers can ethically use cloud computing products in their law practices. But before doing so, it is imperative that they fully assess their ethical obligations and exercise due diligence in vetting their cloud computing provider of choice."[94] In practical terms, reasonable precautions should be taken, except in cases where especially sensitive circumstances require extra precautions.

While there has been a lot of discussion regarding attorneys' professional responsibility obligations of competence and confidentiality in cyberspace, there have been few cases directly litigating this issue.[95] Likewise, although a number of negligence cases have also been brought in the corporate world, few have resulted in successful judgments for the plaintiffs.[96]

The main difficulty in litigating corporate, or attorney, negligence in failing to protect information is the parties' inability to show damages.[97] It

---

91. *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999) (stating that attorneys must consider the sensitivity of information, costs of disclosure, and security of the technology when using the technology to communicate information); Iowa State Bar Association, Committee on Ethics & Practice Guidelines, Op. 11-01 (2011), *available at* http://iowabar.org/associations/4664/files/Ethics%20Opinion%2011-01%20--%20Software%20as%20a%20Service%20-%20Cloud%20Computing.pdf (providing that cloud storage and transmittal is acceptable but requiring attorneys to perform due diligence to determine the degree of protection required based on the client, matter, and information involved).

92. *See* MODEL RULES OF PROF'L CONDUCT R. 5.3 cmt. 3 (2011) (providing the storage of information using an Internet-based service—a form of cloud computing—as an example of non-attorneys outside the firm).

93. MODEL RULES OF PROF'L CONDUCT R. 5.3.

94. Nicole Black, *The Ethics of Cloud Computing for Lawyers*, ABA: GPSOLO EREPORT (Sept. 2012), http://www.americanbar.org/publications/gpsolo_ereport/2012/September_2012/ethics_cloud_computing_lawyers.html.

95. *See generally* Stephanie L. Kimbro, *Practicing Law Without an Office Address: How the Bona Fide Office Requirement Affects Virtual Law Practice*, 36 U. DAYTON L. REV. 1 (2010) (discussing the challenges lawyers face when working online); Shellie Stephens, *Going Google: Your Practice, the Cloud, and the ABA Commission on Ethics 20/20*, 2011 U. ILL. J.L. TECH. & POL'Y 237 (same).

96. *Cf. In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 131 n.128 (D. Me. 2009) (explaining that courts are nearly unanimous in not allowing for recovery when the information that has been stolen has not been misused and only a risk of injury exists), *rev'd in part sub nom.* Anderson v. Hannaford Bros. Co., 659 F.3d 151 (1st Cir. 2011).

97. *See* Allison v. Aetna, Inc., No. 09-2560, 2010 WL 3719243, at *11 (E.D. Pa. Mar.

is difficult to assess damages because of the challenges in answering key questions about cyber security breaches: who perpetrated the cyberattack; what information did they steal; what is the value of that information to them or others; and what other harms, such as operational disruption, competition, or reputational damage, resulted for the victim? Answering these questions has been a challenge for the legal community and for others who need to assess damages, such as insurers, but many in these professional communities are working to improve methods and metrics with which damages can be assessed[98]

As these professionals develop better ways to measure damages, the prevalence of unsuccessful complaints might reverse itself. If that happens, the ethical and professional duties attorneys have to protect their clients by adapting to technology and protecting confidentiality in cyberspace will be upheld more regularly and more stringently.

C. As Companies Become More Aware of Law Firms' Vulnerabilities, Firms Will Have To Change and Strengthen Their Cybersecurity Policies

In the next few years, law firms are likely to experience increasing expectations to establish proactive cybersecurity risk management programs and protect their own and their clients' information.[99] One reason for the push on law firms for internal cybersecurity vigilance is the growing awareness of cyber risks among the public, policymakers, and businesses that patronize law firms.[100] Until recently, awareness of

---

9, 2010) (stating that "Plaintiff's alleged injury of an increased risk of identity theft is far too speculative . . . [and] Plaintiff's allegation that his personal information was even accessed is conjecture"); Pinero v. Jackson Hewitt Tax Serv. Inc., 594 F. Supp. 2d 710 (E.D. La. 2009) (deciding that "plaintiff has alleged only speculative damages . . . has not alleged that any third party accessed her information and stole her identity [and]. . . has not alleged any concrete financial losses resulting from the alleged negligence"); Melancon v. La. Office of Student Fin. Assistance, 567 F. Supp. 2d 873, 877 (E.D. La. 2008) (finding that "the mere possibility that personal information may be at increased risk does not constitute actual injury sufficient to maintain a claim for negligence").

98. *See* Peter Maass & Megha Rajagopalan, *Does Cybercrime Really Cost $1 Trillion?*, PROPUBLICA (Aug. 1, 2012, 11:12 AM), http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion (criticizing the methods adopted by McAfee and Symentec, two anti-virus software providers, when attempting to calculate the global cost of cybercrime).

99. *See* Mandell & Schaffer, *supra* note 12 (describing the emerging liabilities faced by attorneys who fail to protect sensitive data).

100. *See* Jennifer Smith, *Lawyers Get Vigilant on Cybersecurity*, WALL STREET J., June 25, 2012, at B5 (mentioning that the push for cybersecurity vigilance sometimes comes from clients, such as financial institutions who undertake their own security audits at law offices to ensure the safety of sensitive information). Members of Congress will be well aware of problems with cybersecurity since computer hackers have victimized numerous congressional offices. *See* Pete Yost & Lara Jakes Jordan, *Lawmakers Say Capitol Computers Hacked by Chinese*, HUFFINGTON POST (June 11, 2008, 8:11 PM), http://www.huffingtonpost.com/2008/06/11/lawmakers-say-capitol-com_n_106640.html (stating that congressional computers have been the targets of hackers for years).

cyberattacks was shaped largely by headlines about theft of credit card numbers and personally identifiable information.[101]

Increasingly, theft of business secrets and intellectual property is making its way into the public awareness.[102] A 2012 report on legal issues concerning public company directors and corporate general counsel found that, for the first time, a greater percentage of directors (48%) and general counsel (55%) identified data security more than any other topic as an issue of concern.[103] As awareness of the threat and consequences grow, so too will expectations for law firms to act to address the problem. Already, law firms' clients are asking their attorneys to disclose what cybersecurity programs they have in place to protect sensitive information, thus increasing the incentive for law firms to protect their data and perhaps beginning to establish a standard of care for doing so. If law firms begin to lose business because clients decide they cannot be trusted to protect their information, law firms will surely take notice.

Another likely contributing factor for concern is the escalating threat of greater harm to companies. If the consequences of cyber insecurity worsen, pressure to act will grow. For example, the theft of data, with which we are becoming familiar, may become supplemented by the disruption or destruction of data, an action that not only helps competitors but also directly harms a company's own operations. In 2012, the Middle Eastern oil and gas company Saudi Aramco experienced the Shamoon attack, which wiped data—deleted rather than stole it—from the hard drives of 30,000 of the company's computers and kept some networks offline for over a week.[104] If this kind of disruption or destruction of data becomes more common, pressure to improve cybersecurity will increase.

In the face of this growing concern, some law firms are seeking to offer cybersecurity services to their clients.[105] In fact, law firms are claiming a

---

101. *Cf.* Craig Hoffman, *APT Threat Report Shows Cybersecurity Risks Not Limited to Identity Theft*, JDSUPRA (Feb. 2, 2013), http://www.jdsupra.com/legalnews/apt-threat-report-shows-cybersecurity-ri-51290/ (providing that many companies erroneously believe they will not be attacked by hackers because they do not store personal information).

102. *See* Dunn, *supra* note 82 (recognizing intellectual property as a target for hackers).

103. CORP. BOARD MEMBER & FTI CONSULTING, LEGAL RISKS ON THE RADAR: THE CORPORATE BOARD MEMBER/FTI 2012 LAW AND BOARDROOM STUDY 2 (2012), *available at* http://www.fticonsulting.com/global2/media/collateral/united-states/legal-risks-on-the-radar.pdf.

104. *See Shamoon Was an External Attack on Saudi Oil Production*, INFOSECURITY MAG. (Dec. 10, 2012) [hereinafter *Shamoon was an External Attack*], http://www.infosecurity-magazine.com/view/29750/shamoon-was-an-external-attack-on-saudi-oil-production/ (explaining that the Shamoon attack was an external attack on Saudi oil production, which began through spear-fishing aimed at one or more Aramco employees).

105. *See* Catherine Ho, *Jenner & Block Adds Privacy Group*, WASH. POST, Sept. 10, 2012, at A3 (providing that prominent law firms such as Jenner & Block, Venable, Hogan Lovells, and Covington & Burling have moved into the lucrative data and privacy protection practice area).

distinct value to clients in need of cybersecurity services because they can protect sensitive information about clients' cyber risks through attorney-client privilege.[106] To advise clients credibly on cyber risks, breach response, disclosure obligations, and associated liabilities, all while emphasizing the importance of protecting sensitive information, law firms will need to have their own cybersecurity house in order. Cybersecurity may even become a competitive differentiator: law firms that implement best practices and lead the pack in cybersecurity will emphasize this message with prospective clients, incentivizing others to play catch-up with their own cybersecurity. The cumulative effect of all these converging trends may be to establish a standard of care that law firms must implement to protect their own networks and their clients' data.

III. ATTORNEYS WILL HAVE TO IMPLEMENT STRATEGIES TO MITIGATE HARM FROM CYBERATTACKS

A. The Government Has a Limited Set of Tools To Help Fight the Cyberthreat

Having explored the threats, targets, and vulnerabilities of law firms to cyberattacks, we must also seek to answer what law firms can do in the face of this emerging threat. If the nation were under attack, particularly from foreign powers, the government would have an inherent right to protect itself and an obligation to provide for the common defense.[107] However, while many cyber incidents are termed attacks, most are not egregious or damaging enough to warrant a national government response.[108]

This is particularly true when it comes to the theft of intellectual property or business secrets, which is more akin to corporate espionage than warfare. The distinction emerged in outgoing Secretary of Defense Panetta's recent speech on cybersecurity. Secretary Panetta described the Department of Defense's role as a supporting role. He emphasized that it is not the Defense Department's responsibility to provide for the day-to-day security of private and commercial networks.[109] He did, however, note that the Defense Department would be ready to respond if a "crippling cyber-

106. *See* Christopher Matthews, *Law Firms Tout Cybersecurity Cred*, WALL STREET J., Mar. 31, 2013.

107. *See* US CONST. pmbl. (declaring the provision of a common defense as a reason for which the U.S. Constitution was created); U.N. Charter art. 51 (providing that the U.N. Charter does not prohibit the "inherent right" of self-defense).

108. *See* Peter T. Leeson & Christopher J. Coyne, *The Economics of Computer Hacking*, J.L. ECON. & POL. 511, 516–17 (2005) (providing the results of a study that suggest a preponderance of hackers indicated innocuous reasons for their behavior).

109. *See* Panetta, *supra* note 1 (stating that the Department of Defense's mission is to defend the nation and not to monitor individual citizens' computers).

attack" were launched against the United States or if the President ordered him to respond.[110] Things change quickly in cyberspace, and rules governing responsibilities are shifting lines in the sand. Just a few months after Panetta's speech, the National Security Agency is offered to help banks that have suffered disruptive, but certainly not crippling, attacks that took their websites offline for hours or days.[111] This non-emergency assistance shows that the government may be more willing to help than it originally indicated. The Pentagon has suggested it will soon establish more detailed rules of engagement governing cyberattacks and cyberwar, though the extent to which those will be public or will clarify support for the private sector is unclear.[112]

However, many of the domestic statutes that may be used to fight cyberattacks, such as those governing telecommunications, law enforcement, and homeland security in cyberspace, are woefully out of date.[113] This often leaves government with few law enforcement tools outside of investigation for use in helping private companies.[114] In fact, some strategies that could have been used to help, such as sharing information about attacks, can actually violate national security, communications, and privacy laws.[115] While Congress has attempted to update these statutes, change seems unlikely in the current, polarized environment.[116] Thus, the private sector in general must ensure that it has the technology, training, and know-how to defend its own systems from intruders, within the bounds of current law.

B. Managing Cybersecurity Involves More Than Just Managing IT

Facing a persistent threat and limited government help, law firms need to take managing their cybersecurity challenges into their own hands. To

---

110. *Id.*

111. *See* Ellen Nakashima, *Banks Seek NSA Help With Computer System Attacks*, WASH. POST, Jan. 13, 2013, at A3 (stating that major U.S. banks will receive technical assistance from the National Security Administration to assess the banks' systems and understand how hackers were able to disrupt their websites).

112. *See* Ryan Neal, *The Art of War: Pentagon Developing New Rules to Combat Cyberwarfare*, INT'L BUS. TIMES (Apr. 5, 2013), http://www.ibtimes.com/art-war-pentagon-developing-new-rules-combat-cyberwarfare-1174297# (noting that, while the military is developing cyberwafare capabilities, how and whether to respond to attacks on the private sector remain unclear).

113. *See* 18 U.S.C. § 1030 (2006) (creating the Computer Fraud and Abuse Act, making unauthorized access of computers a federal crime, which is almost thirty years old).

114. *See id.* § 1030(d)(2) (granting primary investigative authority under the Computer Fraud and Abuse Act to the Federal Bureau of Investigation).

115. *See* Eamon Javers, *Cyberattacks: Why Companies Keep Their Mouths Shut*, CNBC (Feb. 25, 2013), http://finance.yahoo.com/news/cyberattacks-why-companies-keep-mouths-191414738.html (explaining that companies may be reluctant to publicize data security breaches for fear of incurring legal liabilities).

116. *See* Panetta, *supra* note 1 (criticizing the "legislative and political gridlock" impeding updates to the statutes dealing with cyberspace).

succeed, executive leaders at law firms must realize, as some are beginning to do, that cybersecurity is more than just an IT issue and requires executive management and company-wide engagement. Law firm senior executives have a range of roles to play but foremost among these are treating cybersecurity as a high-priority business risk, establishing a governance framework to manage cybersecurity, and creating a strong culture of cybersecurity among its employees.

First, executives need to learn about cybersecurity threats and make strategic decisions about the risks the company faces: should the firm be more worried about an attack that disrupts its networks so that attorneys lose access to information, about an attack that reveals sensitive data belonging to clients, or about an attack, that exposes the firm's own secret business data? Who are the actors that might pursue each of these attacks? What can the company do to prevent each type of attack or, if the attack happens, to manage its consequences?

Executives also need to make decisions about trade-offs between business needs and cybersecurity. Is the firm willing to make it more inconvenient for traveling attorneys to access their data in exchange for more security, and when does a business imperative make certain actions "worth the risk"? Executives must not only make these decisions but also communicate to the entire firm that cybersecurity is an important business priority for the firm.

Making high-level decisions about risk allows the firm to put in place a strategy to manage its most significant risks and avoid worst-case scenarios; without a risk-based strategy, firms may invest scarce resources protecting against less important harms or trying to defend everything equally, which often means inadequately. Unfortunately, a recent survey revealed that two-thirds of CEOs reported they do not have the information they need to "effectively translate IT security risk into business risk," and law firm management committees no doubt face similar challenges. Much work remains to be done.

Second, law firm executives need to decide how they will manage cybersecurity risk and who will be responsible for what. Different companies use different governance frameworks to manage cybersecurity risk: some establish a cybersecurity committee; others leverage an existing risk management committee; and still others identify one senior officer, frequently a chief information officer, chief operating officer, or chief risk officer, to be the person ultimately accountable to the firm's management or partners.

Regardless of the specific governance model, executives or partners with a range of responsibilities need to be actively involved in managing cybersecurity risk. Managers responsible for Human Resources have an

important role to play in communicating with employees, evaluating adherence to cybersecurity policies, and facilitating training, games, or exercises to promote policies and a cybersecurity culture. Financial managers need to support budgeting for cybersecurity investments. Managers responsible for procurement and third-party contracting should leverage their authorities to improve cybersecurity in the firm's supply chain and among the vendors on whom it depends or with whom it shares information. A key refrain among mature cybersecurity organizations is that cybersecurity is everyone's job.

Third, executive involvement is also essential to establishing a strong culture of cybersecurity, which is a vital asset in managing cyber risk.[117] Establishing a culture of cybersecurity among a firm's employees means explaining why cybersecurity is important and how each employee can and must contribute to the firm's cybersecurity. It also means implementing policies that control cyber risk and supporting those policies with training for employees.[118]

In the cyber age, a single click by a single employee can make the difference between a company that is breached and loses vital information and a company that avoids this fate. Many companies have fallen victim to spear-phishing attacks, for example, in which attackers crafted realistic e-mail communications to employees and induced them to click on a link or attachment that deployed malware within the company's network. Unfortunately, today's technology systems are often unable to detect these attacks and may not protect a company if its employees are not aware and helping to manage the firm's cyber risks. Getting employees to manage cyber risks effectively, though, is challenging and requires executive leadership to emphasize this important responsibility, set an example, and dedicate resources to training and awareness programs. For this reason, even a strong IT department cannot manage cybersecurity alone.

The role of the individual and of culture, policies, procedures, and training are key in avoiding breach. Policies like maintaining effective passwords and not using portable media such as USB drives that can carry malware are truly just the beginning; employees today need to be able to detect spear-phishing attacks, understand how their social media activity

---

117. *See* PRICEWATERHOUSECOOPERS, SAFEGUARDING YOUR FIRM FROM CYBER ATTACKS 7 (2012), *available at* http://www.pwc.com/us/en/law-firms/assets/pwc-safeguarding-your-firm-from-cyber-attacks.pdf (recommending that law firms foment a culture of awareness in their offices through the implementation of training programs and best practices targeting the protection of information).

118. *See* Dunn, *supra* note 82 (discussing a new report by the data security firm Trustwave that argues cybersecurity policies must be accompanied by employee education and security awareness training).

can create cyber risk,[119] and be alert to warning signs of an intrusion.[120] The executives, in turn, must set the strategy and the culture to help the firm and its employees manage the most important cyber risks.

C. IT Still Plays an Important Role in Preventing Cyberattacks

Traditional IT, network security, and technology are still extremely important in preventing cyberattacks. The law firms that stand the best chance of mitigating cyber risk use a risk-based strategy to guide decisions and implement appropriate best practices in technology and network security. These strategies can help prevent attacks or lessen the consequences even where human resources fail.

Technology solutions exist to serve many important functions: blocking malware; detecting anomalous behavior, such as extraction of significant quantities of data off company networks, that can indicate a cyberattack; managing security incidents; and, logging network activity to support forensics.[121] Technology can also facilitate backing up data off-site so that operations and data can be restored in the event of a cyberattack that wipes out files on the company's main network.[122]

Fortunately, many cyberattacks are perpetrated not by the most sophisticated nation-state actors or advanced hacktivists but by hackers or criminals exploiting well-known vulnerabilities that companies have not taken the time to fix.[123] For this reason, proactive network security by a properly resourced IT team can significantly reduce cyber risk.[124] Even if not every attack can be stopped, law firms would reduce their liability by implementing effective network security. One reason for this would be

---

119. *See id.* (explaining that cyberattacks are often initially carried out through the use of spear-phishing and detailing the type of sensitive information that could be revealed through the use of social media).

120. *See* VERIZON, 2012 DATA BREACH INVESTIGATIONS REPORT 62 (2012), *available at* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf (outlining warning signs that indicate a threat is underway); Dan Kaplan, *RSA 2013: Hackers Will Get in, So Spend the Money on Pushing Them Out*, SC MAG. (Feb. 27, 2013), http://www.scmagazine.com/rsa-2013-hackers-will-get-in-so-spend-the-money-on-pushing-them-out/article/282238/ (quoting an information security company's Chief Security Officer, who recommends that companies focus more on recognizing cyberattacks because such attacks can go unnoticed for months).

121. *See* PRICEWATERHOUSECOOPERS, *supra* note 117 (recommending that law firms take six steps to improve their cyber defenses: ensuring leadership is aware of the importance of IT security; installing anti-virus programs; updating filters that intercept undesired e-mail; running programs that detect anomalous activity in the computer system; developing a response plan in case a breach occurs; and providing training programs).

122. *See* Glenn C. McGovern, *Surviving Total Destruction of Your Law Office and Client Base After a Catastrophic Disaster*, 41 TORT TRIAL & INS. PRAC. L.J. 799, 812 (2006) (recommending that law firms also have offsite data backup in case of a natural disaster).

123. *See* VERIZON, *supra* note 120, at 3 (providing that many cyberattacks are unsophisticated and that 97% of breaches could therefore have been avoided through simple or intermediate controls).

124. *Id.*

that, by making themselves less attractive targets, law firms would begin to displace some of the attacks that currently seek them out because they are softer targets than other companies.

D. Post-Breach Strategies Will Help Mitigate Damage After the Inevitable Cyberattack

Even with the most diligent cybersecurity risk management, there is the possibility that a significant cyberattack will happen. If the attackers are sophisticated and persistent enough, they are almost impossible to stop entirely.[125] When a breach does occur, how a law firm manages the response can have a major impact on the eventual liability and damage that arises.

The first step in effectively managing a cyberattack is knowing it happened. Shockingly, breaches were discovered by third parties rather than the breached company in 92% of incidents reported in Verizon's *2012 Data Breach Investigations Report*.[126] The best way to make sure an attack is detected is to have in place the right technology, the right level of awareness among non-IT personnel of what to report, and the right procedures for IT personnel to actively monitor for, detect, and report intrusions.[127]

Once an attack is detected, the goal becomes two-fold: managing the incident itself while maintaining, or in the worst-case scenario restoring, normal operations. In some cases, crisis response can last hours; in other cases, response can last more than a week.[128] Having a well-trained, properly resourced IT security team along with the support of an executive team that understands the fundamentals of cybersecurity incident response can make a major difference in how well a law firm responds to a rapid-fire crisis or a sustained incident.[129]

One helpful response tool for law firms with limited overhead and IT resources is to establish, in advance of a breach, relationships with third-

---

125. *See* Kaplan, *supra* note 120 (arguing that companies cannot prevent cyberattacks and should instead focus their security efforts on detection and breach response).

126. VERIZON, *supra* note 120, at 3.

127. *See* Kaplan, *supra* note 120 (observing that recognition of a breach is vital so that a hacker is quickly caught and thrown out of the network or impeded).

128. *See Shamoon Was an External Attack*, *supra* note 104 (stating that the Shamoon attack left networks offline for over a week); *see also* VERIZON, *supra* note 120, at 3 (asserting that companies usually discover there has been a security breach weeks or months after the initial intrusion).

129. *See* Seth Berman, *Law Firms' Security Requires Rethink*, LEGAL INSIDER, http://www.legaltechnology.com/latest-news/law-firms-security-requires-rethink/ (last visited June 15, 2013) (highlighting that senior partners must understand the importance of a cybersecurity and designate a Chief Technology Officer to oversee security and breach response).

party providers who can make a difference in crisis response.[130] These relationships allow the law firm to enhance or "surge" its capabilities and respond quickly without carrying the costs of a larger IT response team and they may be able to negotiate discounts by establishing relationships in advance rather than waiting until an incident occurs. Law firms should explore relationships with incident response and forensics firms, public relations firms, and consultancies or advisory firms that specialize in helping to manage cybersecurity incidents. Where law firms already have relationships, as many frequently do, they should consider holding discussions or simulations with their vendors to walk through possible scenarios and plan ahead for a real incident.[131]

Perhaps the best way to prepare for the infrequent event of a significant cyber breach is to practice response procedures. Executives and IT security teams can use drills, table-top exercises, and even periodic team meetings to practice the procedures, decision making, and tactical response that will become essential if a significant breach happens.[132]

Firms need to be aware not only of how to mitigate damages but how to mitigate any resulting liability. After a breach, communicating with investors and customers is vital and law firms should plan ahead for how they will manage the liability risks inherent in balancing disclosure obligations to clients or investors with not wanting to share incorrect information before an after-action investigation is complete.[133] While these strategies may be somewhat effective at limiting liability now, as attacks become more frequent and more harmful, how firms respond to them will change.

Although law firms are often at a disadvantage in managing their cybersecurity for the reasons discussed earlier, one inherent advantage they have is that they can learn from the experiences and best practices of other industries with more sophisticated cybersecurity. Companies in financial services and in certain critical infrastructure sectors, in particular, have been wrestling with cyber risks for years and can provide valuable lessons for law firms. By standing on the shoulders of giants, law firms can

---

130. *See id.* (suggesting that a third-party company specializing in post-breach forensic investigation should conduct a post-breach forensic investigation after a security breach).

131. *See* John Leydon, *GCHQ Lines up BAE and Pals for 'Cyber Incident Response:' When Only a Huge, Bloated Military Contractor Can Help*, REGISTER (Nov. 7, 2012), http://www.theregister.co.uk/2012/11/07/gchq_cyber_incident_response_scheme/ (unveiling a plan by the British government to recommend four companies specializing in digital attacks to the nation's critical organizations before any attacks occur in order to "detect attacks early and thwart them before any real damage is done").

132. *See* Berman, *supra* note 129 (claiming that ongoing training is important because it "remind[s] and re-educate[s]" employees and partners about the ever-changing cyber threats).

133. *See* VERIZON, *supra* note 121, at 58–61 (analyzing the impact of data breaches).

accelerate their cybersecurity risk management and therefore become more resilient, less attractive targets for attackers.

CONCLUSION

The escalating cyber risks of recent years show no signs of abating. Law firms have been attractive targets for hackers, and the reputational and liability risks for law firms are likely to increase in the near future as a result of a number of converging factors: new regulations, industry standards, or common practices that establish a standard of care; disclosure obligations;[134] increasing awareness of new and dangerous cyber risks;[135] an ability to quantify the damages caused by cyber incidents;[136] and client expectations.

Fortunately, there is a lot that law firms can do to reduce their risk and liability.[137] In particular, law firms can begin to implement best practices in cybersecurity risk management. Some specific areas could include strategy and governance, training, technology, and network security. Firms can also take a more active role in the current cybersecurity policy discussions at the federal and state levels.

The legal community will no doubt have a defining influence on the evolution of cyber risk and liability across all sectors. To do so responsibly, it should keep pace with how leaders in other sectors are managing cyber risk and apply those lessons internally. For example, the client security practices of the financial services sector and the defensive measures of the national security community could be particularly instructive. Doing so will reduce risk, increase credibility, and provide clients with the level security that they deserve.

---

134. *See supra* note 57 (maintaining that forty-six states have passed data breach notification statutes).

135. *See supra* note 102 and accompanying text (describing how commentary about security breaches no longer solely focuses on identity theft, but has grown to include problems like theft of intellectual property).

136. *See supra* note 98 (proffering that two software security firms have recently attempted to estimate the amount of damage caused worldwide by cyberattacks).

137. *See supra* Part II.B–D (outlining steps law firms can take to reduce the risk of a security breach and potential liability).