VOLUME 23 FALL 2017

ILLINOIS BUSINESS LAW JOURNAL

KEEPING INFORMATION SECURE: THE FEDERAL TRADE COMMISSION'S ROLE IN DATA SECURITY

❖ NOTE ❖

*Brittany Wiegand**

TABLE OF CONTENTS

I. INTRODUCTION 1
II. ANALYSIS 2
A. NIST 6
B. Federal Trade Commission Security Standards 7
1. Authority 8
2. Cybersecurity Watchdog 9
IV. CONCLUSION 11

I. INTRODUCTION

Cybercrime damage costs will hit $6 trillion annually by 2021.[1] This represents the greatest transfer of economic wealth in history and is potentially more devastating than the global trade of all major illegal drugs combined.[2] Given advances in technology, law firms' data security is a growing concern. Though standards and frameworks have been laid out by federal agencies, they do not currently go far enough to adequately protect clients against cyber security threats. Regulations should be codified into law to prevent against the

[1] Steve Morgan, *Top 5 Cybersecurity Facts, Figures and Statistics for 2018* CSOONLINE (Jan. 23, 2018, 8:11 AM), https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html.
[2] *Id.*

*J.D. Candidate, Class of 2020, University of Illinois College of Law.

increasingly advanced capabilities of potential threats. The Federal Trade Commission has enforcement power over companies that fail to take basic precautions, but more needs to be done ex ante to prevent breaches and the loss of valuable information.

Part II of this Note will evaluate the context of current breaches, specifically regarding law firms. Part III will analyze two potential regulatory bodies, the NIST and the FTC, and argue that the FTC is in a better position to regulate to prevent future breaches. Lastly, Part IV will conclude that the FTC can and should promulgate regulation to prevent future security breaches.

II. ANALYSIS

In the past few years, several cyber security attacks targeted at large companies have made headlines, increasing consumer awareness of the importance of cyber security. Equifax, one of the largest credit bureaus in the United States, said in September 2017 that a weakness in an application led to a data breach that exposed approximately 143 million consumers.[3] eBay reported a cyberattack in May 2014 that exposed names, addresses, dates of birth, and encrypted passwords of all its 145 million users. Using the credentials of three corporate employees, the hackers got into the company network and had complete access inside the system for 229 days.[4]

Target Stores' December 2013 breach began before Thanksgiving, but was not discovered until several weeks later.[5] Hackers, gaining access through a third-party HVAC vendor, accessed its point-of-sale payment card readers and collected about 40 million credit and debit card numbers.[6] Yahoo announced in October 2017 that all 3 billion user accounts had been compromised, including personal information, such as names, dates of birth, email addresses, passwords,

---

[3] Taylor Armerding, *The 16 biggest data breaches of the 21st century,* CSO ONLINE (Oct. 11, 2017, 5:31 AM), https://www.csoonline.com/article/2130877/data-breach/the-16-biggest-data-breaches-of-the-21st-century.html.
[4] *Id.*
[5] *Id.*
[6] *Id.*

security questions and answers.[7] These few examples highlight a general need for greater care to be taken with consumer information. Given the highly-sensitive nature of legal work, law firms need to take note and actively protect their systems from potential intrusions.

Law firms hold extremely private and sensitive information, and are not immune from cyberattacks. In 2015, TruShield, an IT security company, reported that the legal industry was the second most targeted sector for a cyberattack.[8] Law firms' data is particularly crucial because their servers hold valuable information, such as businesses' intellectual property, medical records, and bank information. Hackers looking to monetize this information can access a cache of information by breaching a single law firm.[9] The American Bar Association's 2017 *Legal Technology Survey Report* found that twenty-two percent of respondents experienced a cyberattack or data breach at some point, an increase of eight percentage points over the previous year.[10] The ABA Journal argued that cybersecurity was the biggest risk that law firms faced in 2017, and that protecting data is the most critical step all law firms must implement.[11] However, many firms put off taking precautions because they assume they will never be targeted.[12]

Some major law firms have been the targets of attacks: Cravath, Swaine & Moore and Weil Gotshal & Manges, two of the largest firms in the United States,

---

[7] *Id.*
[8] Nabeel Ahmed, *The 4 Biggest Cyber Security Challenges Facing Law Firms Today,* TRUSHIELD (June 22, 2017), https://trushieldinc.com/cnsg-and-trushield-security-solutions-inc-announce-integration-partnership-streamlining-connectivity-and-cybersecurity-solutions/.
[9] *See* Dan Steiner, *Hackers are Aggressively Targeting Law Firms' Data,* CIO.COM (Aug. 3, 2017, 5:38 AM), https://www.cio.com/article/3212829/cyber-attacks-espionage/hackers-are-aggressively-targeting-law-firms-data.html.
[10] Jason Tashea, *Digital Dangers: Cybersecurity and the Law*, ABA J. (Jan. 2018), http://www.abajournal.com/magazine/article/business_law_cybersecurity/.
[11] *Top 6 Cyber-Attacks on Law Firms,* Tritium Information Security (May 11, 2017), https://www.tritium-security.com/single-post/2017/05/16/Top-6-Cyber-Attacks-on-Law-Firm.
[12] *Id.*

were the target of a major cybersecurity breach in 2016.[13] Hackers broke into the files of these firms in an insider-trading scheme that involved planned mergers, and the hackers gained more than $4 million with the information obtained from attack.[14] Evidence from *Fortune* showed that the attacks took place over a ninety-four day period starting in March of 2015.[15] Sources in law enforcement confirmed the role of China in the e-mail hacking campaign.[16] Additionally, DLA Piper was hit by a major cyber attack in 2017, resulting in over 100 million dollars in costs.[17] The ransomware attack originated in an office in Spain, and quickly spread to offices worldwide.[18]

In addition to data breaches from outside sources, the use of personal phones and devices for work increases the ways in which a hacker could obtain private information. The dynamic nature of the problem requires more creative and complex solutions. Federal regulation is lacking,[19] but it plays an important role since it can solve problems that markets cannot solve on their own. Since markets are typically focused on short-term profits, they do not solve collective action problems.[20] Furthermore, historical precedents exist for new technology

---

[13] Julie Sobowale, *6 Major Law Firm Hacks in Recent History,* SIDEBAR, ABA J. (March 2017), http://www.abajournal.com/magazine/article/law_firm_hacking_history.
[14] *Id.*
[15] Jeff John Roberts, *Exclusive: China Stole Data from Major U.S. Law Firms,* FORTUNE (Dec. 7, 2016), http://fortune.com/2016/12/07/china-law-firms/
[16] *Id.*
[17] James Booth, *DLA Piper's Hack Attack Could Cost 'Millions',* LAW J. NEWSLETTERS, (Aug. 2017), http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2017/08/01/dla-pipers-hack-attack-could-cost-millions/.
[18] Debra Cassens Weiss, *DLA Piper hit by 'Major Cyber Attack' Amid Larger Hack Spreading to US*, ABA J. (June 27, 2017, 12:27 PM), http://www.abajournal.com/news/article/dla_piper_is_hit_by_major_cyber_attack_amid_larger_hack_spreading_to_us/.
[19] See *New York's Cybersecurity Regulation Compliance Requirements Go Into Effect,* INSURANCE J. (Aug. 29, 2017), https://www.insurancejournal.com/news/east/2017/08/29/462646.htm.
[20] Sean Michael Kerner, *IBM's Schneier: It's Time to Regulate IoT to Improve Cyber-Security,* EWEEK (Nov. 15, 2017), http://www.eweek.com/security/ibm-s-schneier-it-s-time-to-regulate-iot-to-improve-cyber-security.

usage leading to new government agencies and regulations.[21] The development of cars, airplanes, radio, and television have all led to government regulation.[22]

Since data security and technology are constantly changing and improving, any regulations that would be effective solutions must be applicable to the current problem as well as potential problems arising within the next several months and years. Businesses constantly use data in new ways, and security threats are continuously evolving; therefore, current best practices may not be relevant even six months to one year from the date they are created.[23] Regulations must be flexible to accommodate such change and evolve as technology advances.

III. RECOMMENDATION

Historically, industry-specific regulations have focused on consumer protection in healthcare and finance.[24] The Health Insurance Portability and Accountability Act (HIPAA) instructs the Department of Health and Human Services to promulgate regulations establishing information security standards for the handling of Protected Health Information.[25] It requires covered entities and their business associates to conduct risk assessments and develop plans and procedures to protect against administrative, technical, and physical risks.[26] Similarly, the Gramm-Leach-Bliley Financial Modernization Act of 1999 (GLBA) generally obligates organizations to develop information security plans to address administrative, technical, and physical risks.[27]

These regulations address some data and types of organizations. However, they are not broad enough to affect and protect law firms' clients. To protect data more generally, the scope of the regulations must be broader. Regulatory agencies, such as the National Institute of Standards and Technology and the

---

[21] *Id.*
[22] *Id.*
[23] Fernando M. Pinguelo, *NIST Cybersecurity Framework: Not a Guarantee, but Still a Good Bet Against FTC Action,* 303 N.J. LAW. 44, 44 (2016).
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] Gramm-Leach-Bliley Act, Pub.L. 106-102, § 1811, 133 Stat. 1338, 1338 (1999).

Federal Trade Commission, provide two potential means of addressing cybersecurity within law firms.

A. NIST

In February 2013, President Barack Obama issued an executive order titled "Improving Critical Infrastructure Cybersecurity."[28] Citing the importance of the Nation's critical infrastructure in ensuring the national and economic security of the United States, the executive order prompted the National Institute of Standards and Technology (NIST) to develop a framework for the nation's critical infrastructure.[29] The NIST, founded in 1901, is a part of the Department of Commerce, and is one of the nation's oldest physical science laboratories.[30]

In February 2014, the NIST released a set of industry standards and best practices that "assist organizations in identifying, protecting, detecting, responding to, and recovering from cybersecurity risks."[31] The framework developed by the NIST does not create new standards; rather, it was created through collaboration between the government and the private sector, and is based on existing practices and guidelines.[32] Employing common, easily understood language, the framework can be understood by those outside of information technology (IT departments).[33] Updated in December 2017, the framework "uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs, without placing additional regulatory requirements on businesses."[34] The framework is organized into five functions: identify, protect, detect, respond, and recover.[35]

---

[28] Exec. Order No. 13,636, 78 FR 11737 (Feb. 12, 2013).
[29] *Id.*
[30] NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY, https://www.nist.gov/about-nist (last visited Jan. 10, 2018).
[31] Pinguelo, *supra* note 10, at 45.
[32] *Id.*
[33] *Id.*
[34] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, CYBERSECURITY FRAMEWORK (2017).
[35] *Id.*

The framework encourages organizations to improve cybersecurity risk, regardless of size, degree of risk, or sophistication. The text states,

> "Ideally, organizations using the framework will be able to measure and assign values to their risk *along with* the cost and benefits of steps taken to reduce risk to acceptable levels. The better an organization is able to measure its risk, costs, and benefits of cybersecurity strategies and steps, the more rational, effective, and valuable its cybersecurity approach and investments will be."[36]

Although the framework is helpful to organizations seeking to reduce cybersecurity risks, including law firms, its utility depends on a firm's willingness to thoroughly employ the strategies given within the framework.[37] The NIST Cybersecurity framework is merely a starting point.[38] The framework assists organizations interested in seeking protection from cybersecurity threats.[39] It is not an end in itself, since it does not contain specific "requirements, practices, or elements" that must be implemented.[40] Furthermore, because of the threat of new advances in technology, the framework is something that must be constantly revisited in light of new technologies. Though the framework provides helpful guidance, it does not go far enough in ensuring clients' data since it does not provide mandates for firms. Though the NIST has the potential to regulate the field, another stands in a better position to provide meaningful guidance and enforce penalties.

B. Federal Trade Commission Security Standards

The FTC as a regulatory agency is in a position to provide guidance and enforce penalties for firms. The Federal Trade Commission is the primary federal data security regulator in the US.[41] The FTC is the only federal agency with both consumer protection and competition jurisdiction in broad sectors of the

---

[36] *Id.*
[37] Pinguelo, *supra* note 10, at 45.
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id*.

economy.[42] Section 5 of the FTC Act provides the FTC with broad authority to protect consumers from unfair or deceptive trade practices in or affecting commerce (15 U.S.C. § 45(a)(1) and (2)).[43] Section 5 provides the FTC with three categories of authority: investigation, enforcement, and litigation.[44] Section 5 applies to most companies and individuals that do business in the United States,[45] thus providing potential regulations for law firms to ensure the security of their private information and their clients' data.

1. Authority

Section 5 does not explicitly discuss data security or the authority to enforce inadequate data practices.[46] However, the FTC's authority had, until recently, not been challenged.[47] Companies chose to settle rather than litigate FTC actions against them. However, *Wyndham Wordwide Corp* and *LabMD* are two major exceptions; both challenged the FTC's authority in separate cases.

In 2012, the FTC alleged that Wyndham engaged in unfair trade practices by not employing appropriate measures to protect unauthorized access, breaches, and deceptive trade practices.[48] Wyndham represented to customers that it had implemented reasonable and appropriate measures to protect personal information when it had not done so.[49] In its response, Wyndham asserted that the FTC did not have authority under Section 5 to establish data security standards for the private sector and that it cannot exercise authority under Section 5 to regulate data security without first setting out regulations regarding data security based on traditional principles of fair notice.[50] The district court denied Wyndham's motion and rejected its claims, ruling that the FTC does not need to issue regulations before bringing enforcement actions and rejected the challenge to the FTC's

---

[42] ABOUT THE FTC, https://www.ftc.gov/about-ftc (last visited Jan. 10, 2018).
[43] Pinguelo, *supra* note 10, at 46.
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 236 (3d Cir. 2015).
[49] *Id.*
[50] *Id.*

authority.[51] The court also found that other federal laws complemented rather than precluded the FTC's authority to regulate unfair and deceptive practices in the area of data security.[52] The U.S. Court of Appeals for the Third Circuit affirmed the lower court's decision.[53]

The FTC filed a claim against LabMD after an insurance report allegedly containing personal information of over 9,000 clients was made available on an internet file-sharing network.[54] LabMD's motion to dismiss alleged that the FTC lacked authority to address private companies' data security practices as unfair, among other claims.[55] When LabMD sought relief in courts, the District Court and U.S. Court of Appeals for the Eleventh Circuit both rejected LabMD's claims as premature, since LabMD had not exhausted its administrative remedies and obtained a final FTC agency action. Additionally, the Eleventh Circuit did not address any of LabMD's substantive arguments regarding the FTC's actual enforcement authority.[56]

Despite a few challenges, the FTC has been successful in many enforcement actions against companies.[57] Thus, firms will likely not be able to escape the enforcement power of the FTC. Assuming the FTC has authority over law firms, the question becomes: is the FTC an effective regulator of cybersecurity in law firms?

2. Cybersecurity Watchdog

Assuming the FTC has regulatory power, how effective is the FTC in addressing and preventing attacks within law firms? FTC's data security complaints typically fall into three overlapping categories, including: complaints against organizations for inadequate security practices contributing to a data

---

[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] LabMD, Inc. v. F.T.C., 776 F.3d 1275, 1275 (11th Cir. 2015).
[55] *Id.*
[56] *Id.*
[57] *See, e.g.*, In the Matter of Oracle Corp., No. 132 3115, 2016 WL 1360808 (F.T.C. Mar. 28, 2016). *See also* In the Matter of ASUSTeK Computer, Inc., No. 142 3156, 2016 WL 807981 (F.T.C. Feb. 22, 2016).

breach, complaints against companies for misrepresenting security practices, and complaints alleging security deficiencies in mobile applications.[58] The FTC's 2015 Start with Security, A Guide for Business: Lessons Learned from FTC Cases outlines ten steps companies can and should take in order to ensure data security.[59] The lessons, written in common language, such as "Don't use personal information when it's not necessary," explain the lesson in the context of past FTC cases and allegations, while offering actions to implement in order to prevent a breach.[60] Though the lessons lack technical specificity, they do provide guidance that businesses may consult when developing data security programs.

In 2016, The FTC linked the Start with Security initiative and reasonableness standard to the voluntary NIST Cybersecurity Framework, aligning them, since both require organizations to assess and manage data security risks in the context of their own business. Though helpful for businesses seeking to develop a cybersecurity program, they are limited in their effectiveness because they are voluntary standards.

Businesses interested in protecting information will likely find the guidelines helpful. However, the onus is on the business or firm to do so. If a business fails to recognize the need for data security or chooses to forego the cost, their clients and information are at risk. Enforcement actions from the FTC could punish the business, but they fail to prevent the initial breach unless the firm takes it upon itself to take the steps within the Framework and constantly remain attuned to potential technological developments.

Additionally, the FTC's data security standards do not provide a strict blueprint, rather, they typically "describe the security safeguards the FTC requires using non-specific terms like 'reasonable,' 'appropriate,' 'adequate,' or

---

[58] FTC Data Security Standards and Enforcement, Practical Law Intellectual Property & Technology, Westlaw 8-617-7036.
[59] Fed. Trade Comm'n, Start with Security, A Guide for Business: Lessons Learned from FTC Cases (June 2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[60] *Id.*

'proper.'"[61] Firms seeking to use the standards may struggle if more specific guidance is not given.

Though the FTC can regulate cybersecurity for law firms, stronger guidance is needed on the front end to ensure data security. The framework and standards should be codified in law so that businesses must meet minimum requirements. Enforcement actions happen after a breach has already occurred; firms' data security requires an earlier, more proactive approach that could prevent breaches in the first place. One potential solution is moving in a similar direction to the European Union, which is requiring that firms disclose data breaches to clients.[62] By requiring disclosure and increasing transparency, businesses, policy makers and consumers would be able to make more informed decisions about how to manage cyberrisk.[63] If a company's stock price and/or reputation are on the line, they would be more likely to take preventative action, ideally preventing future attacks.

European law firms face increased scrutiny because the European Union's General Data Protection Regulation, going into effect in May 2018, will require law firms based in the EU as well as those with EU clients to disclose data breaches to clients. TechCrunch reported that Equifax's case could have resulted in a fine of around $62.9 million dollars if it had not reported the data breach it experienced multiple weeks sooner.[64]

IV. CONCLUSION

Computer security firm Fortinet predicts that 2018 will be the year that malicious software becomes even smarter and ransomware becomes more

---

[61] *Id.*
[62] Grubb, *infra* note 10.
[63] Denise Zheng, *YES: Companies Now Are Flying Blind When Closing Security Gaps*, WALL ST J. (May 22, 2016, 10:00 PM), https://www.wsj.com/articles/should-companies-be-required-to-share-information-about-cyberattacks-1463968801.
[64] Natasha Lomas, *Equifax Breach Disclosure Would Have Failed Europe's Tough New Rules*, TECHCRUNCH (Sep. 8, 2017), https://techcrunch.com/2017/09/08/equifax-breach-disclosure-would-have-failed-europes-tough-new-rules/.

targeted and prevalent among big business.[65] Derek Manky, global security strategist, predicts:

> "We predict that cybercriminals will begin to combine artificial intelligence technologies with multi-vector attack methods to scan for, detect, and exploit weaknesses in a cloud provider's environment. The impact of such attacks could create a massive payday for a criminal organization and disrupt service for potentially hundreds or thousands of businesses and tens of thousands or even millions of their customers."[66]

Law firms have a financial and ethical obligation to counter cyberattacks and protect their data.[67] Furthermore, firms have ethical rules requiring confidentiality of attorney-client and work product data.[68] In addition to the highly private nature of law firm data, law firms have ethical obligations to their clients, necessitating an even higher level of data security.[69] The FTC stands in a unique position as the main federal data regulator in the United States, and should promulgate rules mandating minimum standards for law firms.

---

[65] Ben Grubb, *'Swarm' Cyber Attacks, Crypto-Currency Stealing Malware Predicted for 2018*, THE SYDNEY MORNING HERALD (Jan. 8, 2018, 11:15 AM), http://www.smh.com.au/technology/innovation/swarm-cyber-attacks-crypto-currency-stealing-malware-predicted-for-2018-20180107-p4yyaz.html.
[66] *Id.*
[67] Model Code of Prof'l Conduct r. 1.6 (Am. Bar. Ass'n 2015).
[68] *Id.*
[69] *Id.*