DATA BREACH RISKS FOR LAW FIRMS

Pierre Grosdidier
Haynes and Boone, LLP
1221 McKinney Street, Suite 2100
Houston, Texas 77010

Elizabeth Rogers
Greenberg Traurig, LLP
300 West 6th Street, Suite 2050
Austin, Texas 78701

State Bar of Texas
ANNUAL MEETING
June 22–23, 2017
Dallas, Texas

Friday, 10:30 a.m.

Pierre Grosdidier
Haynes and Boone, LLP
1221 McKinney Street, Suite 2100
Houston, Texas 77010
713.547.2272

BIOGRAPHICAL INFORMATION

Education

B.Eng., Chemical Engineering, McGill University, 1980, with distinction
Ph.D., Chemical Engineering, California Institute of Technology, 1986
J.D., University of Texas at Austin School of Law, 2007, with honors

Professional Activities

Pierre Grosdidier worked as a consulting engineer for 18 years before becoming a lawyer. He now leverages his engineering, computer, and business background to litigate cases that involve complex technical and commercial disputes. In 2017, Pierre became Board Certified in Construction Law by the Texas Board of Legal Specialization. Pierre is at ease with the most complex technologies whether in the energy, construction, computer, or manufacturing industries. He has represented clients in lawsuits and arbitrations that arose from construction defects, industrial accidents, environmental contamination, oil and gas drilling operations, engineering services projects, computer and software projects, copyright and software copyright infringements, computer piracy, and trade secret thefts. Pierre's litigation experience also includes claims under the Stored Communications Act and the Computer Fraud and Abuse Act, including one where the defendant planted a "time bomb" in his employer's computer system. Pierre leverages his software and project management experience to efficiently organize and lead complex ESI preservation, collection, and review projects. He is a prolific writer.

Selected Publications

- *Data Breaches, Big Data, and FTC Oversight, presenter, InfraGard Health Care SIG, Sept. 1, 2016.*
- *Admissibility and Authentication of Electronic Evidence, presenter, 2016 State Bar of Texas Annual Meeting, June 17, 2016.*
- *A Modern Whodunit: Non-compliant DMCA § 512 'Takedown' Notifications Might Prevent a Copyright Owner from Learning an Alleged Infringer's Identity, State Bar of Texas, Computer and Technology Section's Circuits Newsletter, September 2, 2015.*
- *Three Threshold Questions Every Attorney Must Answer before Filing a Computer Fraud Claim, Excerpted from Circuits – Newsletter of the Computer & Technology Section Summer 2015.*
- *Don't Look To SCA in BYOD-Termination Remote Wipe Cases, Law360, Mar. 17, 2015.*
- *When Employees Leave with Electronic Files: The CFAA's Eclectic Damage and Loss Case Law Illustrated, co-author, Bloomberg BNA Electronic Commerce & Law Report, May 21, 2014.*
- *When Hacking an Email Account Doesn't Violate the SCA, Law360, Dec. 11, 2013; updated Nov. 3, 2016.*
- *Pitfalls Await Those Who Do Not Think Through TTLA Claims, guest author, Law360, Oct. 15, 2013.*
- *Choose Your Friends – and Privacy Settings – Wisely, guest author, Law360, October 2, 2013.*
- *The Danger With Time Bombs - Can Your Software Vendor Lock Up Your Software so That You Have to Buy an Upgrade? Maybe not, ControlGlobal.com, October 2011 (Updated, Oct. 1, 2015).*

See all P. Grosdidier's publications at http://www.haynesboone.com/people/g/grosdidier-phd-pierre
Disclosure: parts of this article are based on material drawn from some of the above publications.

Elizabeth Rogers
Greenberg Traurig, LLP
300 West 6th Street, Suite 2050
Austin, Texas 78701

BIOGRAPHICAL INFORMATION

Education

J.D., St. Mary's University School of Law, 1988
B.A., The University of Texas at El Paso, 1983

Professional Activities

Elizabeth C. Rogers' wide-ranging experience, including her role as the first Chief Privacy Officer in Texas state government, places her in a very small percentage of law firm business lawyers. In that role, Elizabeth acquired first-hand experience providing practical legal services for cybersecurity and privacy requirements and collaborated with executive leadership, the Office of General Counsel and other stakeholders to develop the state's first official Privacy Division. She also served on the breach response team and responded to numerous security incidents.

Today, her practice draws from her wide-ranging internal experience, but also includes supporting breach responses, privacy risk assessments and technology transactions across industry. Elizabeth frequently speaks and publishes on topics trending in the business community about privacy and cybersecurity.

Selected Publications

- *Seven Privacy Tips & Recent Developments in Honor of Privacy Day, co-author, GT Alert, January 27, 2017*
- *Checklist – Drafting a Breach Notification Letter, Lexis Practice Advisor, December 1, 2016*
- *Checklist – Preparing a Data Breach Avoidance & Response Plan, Lexis Practice Advisor, December 1, 2016*
- *Checklist – Reviewing & Drafting Privacy Policies, Lexis Practice Advisor, December 1, 2016*
- *Drafting Privacy Policies, Lexis Practice Advisor, December 1, 2016*
- *Key Privacy and Data Security Considerations When Negotiating or Reviewing a Transaction or Agreement, Lexis Practice Advisor, December 1, 2016*
- *Planning for & Managing a Data Breach, Lexis Practice Advisor, December 1, 2016*
- *Preparing a Breach Notification Letter, Lexis Practice Advisor, December 1, 2016*
- *Sample Breach Notification Letter, Lexis Practice Advisor, December 1, 2016*
- *Tax Reporting Laws Raise Privacy Claim Risks for Online Companies, co-author, Corporate Counsel, August 1, 2016*
- *Planning and Managing Data Breach and Drafting Privacy Policies, editor, IP & Technology Chapter, Lexis Practice Advisor, 2015*
- *Top Tips For Data Breach Readiness And Response, co-author, Law360, March 25, 2015*
- *Austin's new dealmakers and litigators: Elizabeth Rogers, the data defender, featured, Austin Business Journal, January 23, 2015*
- *How to Prepare for B*reach *Readiness* and Breach Response*, Circuits, Volume 3, Winter 2015*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes and Rules

Secondary Sources

DATA BREACH RISKS FOR LAW FIRMS

I. INTRODUCTION

The term "data breach" usually brings to mind the much-publicized capture of vast quantities of consumer information from retail vendors (*e.g.*, Target, Windham), on-line service providers (*e.g.*, Yahoo!), or social media sites (*e.g.*, Ashley Madison). Hackers' motives are presumably as diverse as the hackers themselves, but clearly include obtaining marketable information, such as credit card numbers and intellectual property, or embarrassing consumers, as in the Ashley Madison breach. Recent events also show that motives now possibly include political agendas with media reports that foreign hackers may even attempt to influence U.S. elections. Of course all this activity is criminal. "Guccifer," the Romanian hacker involved in the disclosure of Hillary Clinton's private email server when she served as Secretary of State, was extradited from his home country and recently sentenced to 52 month of prison after a plea bargain.[1]

As this article shows, law firms are also prime data breach targets because they too hold vast quantities of commercially valuable information in their stores. For example, law firm servers harbor patent applications, merger and acquisition information, and litigation work-product, all of which might make hackers and their sponsors very rich. This article first explores why hackers target law firms and what are counsel's obligations in light of this threat. The article then explores the consequences of a data breach in terms of the potential civil litigation and government enforcement actions. Finally, the article lists some of the tangible steps that a firm can take to protect itself from breaches and the consequences thereof.

II. THE THREAT: WHY LAW FIRMS GET HACKED

A. Cyberthieves are attracted to the proprietary and confidential information that is collected and stored by law firms

Law firms store a wealth of sensitive and confidential information electronically, making them prime targets for hackers. Not only does weak data security affect business development and threaten client retention for firms, but it can result in legal and ethical violations as well. Law firms are targets of immense interest because law firms broker transactions that can have significant consequences on publicly traded companies and they manage litigation involving extremely confidential and regulated data about consumers that can be sold on the dark web. Hackers are able to penetrate webservers and email servers through unauthorized access to credentials, thus allowing a hacker to read emails containing non-public financial information like the price of shares of stock involved in merger discussions. This type of proprietary "insider trading" information can then be easily monetized by merely trading on Wall Street. This is substantively what happened to two law firms with offices in New York City, and led to the December 2016 indictment of three Chinese nationals for insider trading based on information hacked from these law firms.[2] The transactions netted the hackers millions of dollars. Threat actors can also get information from court filings, which are public record. Somebody can jump on Pacer and find out the name of the case and the attorney of record. They can then send an email message that purports to come from the attorney of record using a bogus email address or a fake domain and say "Here's an updated complaint in such and such a case." An unsuspecting and untrained adverse counsel will recognize the email and click on the attachment because this occurs in the normal course of business every week of the year. Through this threat vector, the cybercriminal then can successfully download the ransomware malware that can launch an attack that locks all files it can find within a network.

---

[1] *See http://www.reuters.com/article/us-usa-cyber-guccifer-idUSKCN1175FB.*

[2] *See https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-arrest-macau-resident-and-unsealing-charges-against.*

Finally, because most litigators now file pleadings and discovery electronically, cyber thieves have begun to hack the networks and systems of courthouses, which have paltry budgets for mitigating cyber-crimes. Law firms that have filed certain documents with redacted information, in response to discovery occurring in high stakes litigation, are then targeted for a cyber-attack in hopes that original copies of the redacted documents contain secrets and confidential information that will yield a profit on the dark web.

B. The law firm Culture historically has not fostered physical security and information security of electronic confidential client and firm data

1. Weak cybersecurity profile

Cyberattacks against law firms may not seem to be as epidemic as they are against financial institutions, but if things hold true to form, that may be only because of a lack of awareness or visibility into the state of the law firm's information technology security. Although the IT departments of many global law firms are becoming more sophisticated (mostly because of the history of the EU's omnibus directives and the pending Global Data Protection Regulations, most law firm leaders are historically poor judges of their cybersecurity posture, and their ability to detect breaches is generally poor. The time between compromise and detection is usually measured in months. Because of this is the status quo, law firms are seen as high-value targets for the rapidly growing use of ransomware and other extortion schemes because they have historically weak defenses and are seen as willing to pay large sums.

a. Examples of weak information security practices include:

i. Devices. Common events like misplacing thumb drive, leaving a laptop on the phone, losing an iPhone in a cab, all create vulnerabilities.

ii. Desktop and workstation security. Law firms should have strict and enforced protocols to lock such stations when personnel are not working actively on them.

iii. Vendors. HVAC, facilities and other outside physical vendors that come on site to law firms pose risks if not evaluated in advance for security.

iv. Extranets and litigation support software platforms. Even if a vendor of such services proclaims to offer security, the law firm must still strictly assess and convey the minimum standard requirements for security.

v. Loose password protection.

vi. Lack of encryption.

vii. Remote access.

viii. Access controls to data. There must be controls in place and protocols for access to data, which requires assigning value and categorization to data that the law firm is responsible for storing and processing.

There are easy resolutions to the above issues that do not require technical investment or extensive staff training.

Even after the FBI warned several "Biglaw" managing partners of cyber threats in 2011, changes to improve security postures have not been instituted. Only a few firms have adopted the ISO/IEC 27001 standard and primarily only at the behest of their large financial institution clients. The following are some of the elements of the legal industry, particularly in medium and large law firms, that have created this situation:

2. Business Model

The fiscal culture of the business of law has historically not prioritized financial investment in the area of cybersecurity preparedness. While this is slowly changing in some of the mega-firm models and at some progressive, mid-sized firms, law firms are designed to maximize profit while delivering the highest quality legal services under extreme cost pressures by in-house counsel. These services are delivered in a model that primarily supports an hourly fee structure. Real estate is by far the largest overhead expenditure for most law firms and managing real estate costs generally takes priority over other initiatives.

An effective cyber-risk program, for any size law firm, can be very expensive. Even the simple step of updating software with a patch can be expensive depending upon the terms of the software license.

Another cultural aspect of all size law firms is the attribute of self-regulation and the "group practice" mentality. Defending against cyber threats is a multi-disciplinary effort that requires an enterprise-risk approach. The concept of enterprise risk is generally anomalous to law firms. Many firms operate as a group of partners with equity sharing agreements and a common logo. They do not share many clients or business services, so the issue of enterprise risk and mitigation is not top of mind to partnerships or executive committees in the operations of the firm.

Partners own the firm and often – not always – operate their practices as discrete businesses. Despite putting controls, internal policies and procedures in place, if a senior partner doesn't want to follow them, he or she doesn't have to.

For example, if the IT director announces that all devices will require enhanced security such as tokenization or mandatory password protection, a partner may opt out, as simple as that. These "holes" exist across law firms thereby increasing vulnerabilities – even the least sophisticated hackers may be able to affect a damaging information compromise.

While many of us are grateful for the autonomy our profession has, from the prescriptive scrutiny of an outside regulatory body, this leads to the negative consequence of each attorney doing things according to his or her own code of conduct. Thus, even though taking short cuts are discouraged, in the context of manipulating safeguards meant to protect proprietary and confidential data during electronic and/or wifi transmission, lawyers do so any way. Furthermore, it is not uncommon for several practices within the same law firm to manage information security differently. Expecting all lawyers within the same office and/or multiple offices to maintain a consistent code of conduct is a challenge regardless of the topic, but especially in electronic delivery of legal services.

III. ATTORNEYS' DUTIES UNDER THE PROFESSIONAL RULES AND RECENT EXPECTATIONS OF TECHNICAL FAMILIARITY

A. The American Bar Association's Ethical Duty of Technology Competence

The increasing number of law firm data security threats create certain ethical obligations for lawyers. The framework for analyzing the conduct of lawyers in response to these threats has been borrowed from either the ABA Model Rules governing technology competence or ethical rules closely following them.

1. Understanding ABA Model Rule 1.1: Comment 8

In 2012, the American Bar Association formally approved a change to the Model Rules of Professional Conduct that states that lawyers have a duty to be competent not only in the law and its practice, but also in technology. The ABA's House of Delegates voted to amend Comment 8 to Model Rule 1.1, which pertains to competence to read as follows:

> Maintaining Competence
> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)[3]

There are three components to the Comment 8 duty: i) the first component of the duty is the requirement that lawyers understand the responsibility to properly manage privacy and data security; ii) the second component requires that lawyers understand how to best leverage technology to serve clients, whether it's using a cloud-based collaborative platform more easily or with trial technology to better facilitate efficient use of trial exhibits; and, (iii) the third component requires the lawyer to understand the technology the client is using.

2. Texas Disciplinary Rules of Professional Conduct

To date, twenty-seven states[4] have passed some version of Comment 8. Although Texas has yet to adopt Comment 8, the current Texas Disciplinary Rules of Professional Conduct have been relied upon by the Professional Ethics Committee of the State Bar of Texas in two opinions questioning the ethical propriety of the conduct of Texas lawyers using technology. The Rules implicated are:

a. Rule 1.01 Competent and Diligent Representation

> (a) A lawyer shall not accept or continue employment in a legal matter which the lawyer knows or should know is beyond the lawyer's competence, unless:
>
> (1) another lawyer who is competent to handle the matter is, with the prior informed consent of the client, associated in the matter.

b. Rule 1.05 Confidentiality of Information

> Rule 1.05(b) provides that, except as permitted by paragraphs (c) and (d) of the Rule:
>
> "a lawyer shall not knowingly: (1) Reveal confidential information of a client or former client to: (i) a person that the client has instructed is not to receive the information; or (ii) anyone else, other than the client, the client's representatives, or the members, associates, or employees of the lawyer's law firm.

---

[3] *See http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1.html.*

[4] *The Ethical Duty of Technology Competence has been passed in the following states: Arkansas, Arizona, Connecticut, Colorado, Delaware, Florida, Idaho, Illinois, Iowa, Kansas, Massachusetts, Minnesota, New Hampshire, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Tennessee, Utah, Virginia, Washington, West Virginia, Wisconsin, Wyoming.*

3. Opinions of the Professional Ethics Committee of the State Bar of Texas

The Texas Professional Ethics Committee has recently published Opinions No. 648 and 665 which both question a lawyers' professional conduct and ethical duties arising from the use of technology. Both Opinions (i) involve the transfer of confidential client data via technology, (ii) conclude that the rules impose a duty on lawyers to use the most appropriate technology available to transfer confidential client data, and (iii) use a "reasonableness" under the circumstances test to determine whether the lawyer violated the Rules.

a. Opinion No. 648 (April 2015)

Material Question Presented:

Under the Texas Disciplinary Rules of Professional Conduct, may a lawyer communicate confidential information by email?

Facts:

Most of a law firm's written communication is delivered by web-based email, such as unencrypted Gmail.

Conclusion:

Email communication is proper. Considering the present state of technology and email usage, a lawyer may generally communicate confidential information by email.

Discussion:

Some circumstances, may, however, cause a lawyer to have a duty to advise a client regarding risks incident to the sending or receiving of emails arising from those circumstances and to consider whether it is prudent to use encrypted email or another form of communication. The risk an unauthorized person will gain access to confidential information is inherent in the delivery of any written communication including delivery by the U.S. Postal Service, a private mail service, a courier, or facsimile. Persons who use email have a reasonable expectation of privacy based, in part, upon statutes that make it a crime to intercept emails.

b. Opinion No. 665 (December 2016)

Material Question Presented:

What are a Texas lawyer's obligations under the Texas Disciplinary Rules of Professional Conduct to prevent the inadvertent transmission of metadata containing a client's confidential information?

Facts:

Lawyer A represents a client in the settlement of a civil lawsuit. Lawyer A sends a draft settlement agreement to opposing counsel, Lawyer B, as an attachment to an email. The attachment includes embedded data, commonly called metadata. This metadata is digital data that is not immediately visible when the document is opened by the recipient of the email but can be read either through the use of certain commands available in word-processing software or through the use of specialized software. In this case, the metadata includes information revealing confidential information of the client of Lawyer A related to ongoing settlement negotiations. Lawyer B has no reason to believe that Lawyer A intended to include this metadata in the attachment.

Conclusion:

A lawyer's duty of competence in Rule 1.01 requires that lawyers who use electronic documents understand that metadata is created in the generation of electronic documents, that transmission of electronic documents will include transmission of metadata, that the transmitted metadata may include confidential information, that recipients of the documents can access metadata, and that actions can be taken to prevent or minimize the transmission of metadata.

Lawyers therefore have a duty to take reasonable measures to avoid the transmission of confidential information embedded in electronic documents, including the employment of reasonably available technical means to remove such metadata before sending such documents to persons to whom such confidential information is not to be revealed pursuant to the provisions of Rule 1.05.

Discussion:

Commonly employed methods for avoiding the disclosure of confidential information in metadata include the use of software to remove or "scrub" metadata from the document before transmission, the conversion of the document into another format that does not preserve the original metadata, and transmission of the document by fax or hard copy.

4. State Bar of California Standing Committee on Professional Responsibility and Conduct-Opinion No. 2015-193

A 2015 State Bar of California ethics opinion has been relied on as the "gold" standard as it relates to the Comment 8 duty. It requires attorneys who represent clients in litigation either to be competent in eDiscovery or, if not, associate with others who are. The opinion expressly cites the ABA's Comment 8 and states:

An attorney lacking the required competence for eDiscovery issues has three options: (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation.

While these choices were applied in the context of eDiscovery in the California ethics opinion, they can be applied generally in all instances that question whether the ethical duty of technology competence has been satisfied.

5. Federal Court Decision

In 2014, A federal district court judge in Ohio issued an opinion that provides additional insight into the judiciary's expectations of a lawyer's technology competence in *Brown v. Tellermate Holdings, Ltd.*[5]. There, Judge Kemp imposed severe sanctions against a defendant who had not properly identified or and preserved cloud-based data that would have been important to the case. The court ordered the sanctions based on counsel's affirmative duty to speak to Tellermate's stakeholders so that counsel and client together could identify, preserve, and search the sources of discoverable information. The Tellermate decision demonstrates that technology competence requires lawyers to have at least a base-level understanding of client data and systems. Further, it may be necessary to engage internal or external experts, who understand how the systems work and how data is stored to achieve the required level of technology competence for the client's project.

[5] *Brown v. Tellermate Holdings Ltd., 2014 WL 2987051 (S.D. Ohio July 1, 2014).*

B. What Does It Mean to Be "Competent"?

Satisfaction of the ethical duty of technology competence, in accordance with Comment 8, will likely depend on the task in front of the attorney. At a minimum, it is important that lawyers be able to at least stay informed with the evolution of technology, generally and as it relates the businesses of the client. An attorney who represents environmental businesses, for example, should be familiar with emerging environmental technologies. Likewise, a litigator should know what types of technologies are available to help with large scale document reviews or assessments and collection of documents. The size of the law firm will probably not determine the scope of technology competence so solo and small law firms must be prepared to assume the obligation, under the surrounding circumstances, while a large global firm will also be required to take actions based on surrounding circumstances. Although the actions of each firm will differ, it will be because the minimum standard for each firm will differ. But there will be a minimum standard for each size firm. Specific Steps to Meet Competence Requirements

Some specific steps attorneys can take to ensure they are meeting the technology competence requirements under the Model Rules or state rules include:

a. Understand how computers create, process, collect and maintain information, including understanding the clients system and the difference between the internal memory of the computer and the preservation of data externally, either on a hard drive or on a cloud. It would also involve knowing how to search the client's network and systems for responsiveness so that the lawyer is sufficiently informed to make a decision about whether the client has the capacity to conduct eDiscovery in-house or whether a third-party vendor is needed.

b. Be familiar with the firm's and the client's cybersecurity setup. This includes knowing how the systems are structured, who is responsible for the systems and how hacks are prevented.

c. Know what to do if there has been a breach. If there is a data loss that occurs through a cloud provider, the lawyer should know what the responsibilities are for informing the client and law enforcement.

d. Be Proactive and Self-Aware. Bringing new technologies into the firm is one way for lawyers to raise the level of technical competence. Attorneys should understand the technological tools available and how to use technology to maximize effectiveness and the ability to be the best advocate possible. It is also important for attorneys to be self-aware as it relates to the ability to recognize whether someone with more expertise should be associated to handle the technology issues that are material to the client matter.

1. Realms Where Competency Is Necessary

The duty of technology competence is clearly applicable in the context of protecting client information and cybersecurity but it also applies in several other contexts.

a. Technology Used to Run a Practice and Safeguard Client Information

Although a granular level of understanding is probably not required, to satisfy the ethical duty of technology competence, a lawyer must be familiar enough with cybersecurity and the dangers to confidential client data to be able to assure the client in good faith that the lawyer will keep it secure using reasonable efforts to prevent it from being stolen or hacked. Lawyers who are unfamiliar with standards for measuring the adequacy of information security and privacy may rely on third parties so long as the lawyer takes reasonable steps to make sure that the third party has adequate information and knowledge and technical skills to assess the vulnerabilities.

For lawyers whose practice involves cybersecurity, however, the standards for satisfying the duty of competency in technology will likely be much higher than for attorneys specializing in other practice areas. is very high. For example, in the course of providing legal advice following a cyber-attack, the attorneys who are engaged must understand the client's information technology infrastructure, the technology implicated, and how the cyber-attack occurred.

b. Client Technology

The ethical duty of technology competence also requires the lawyer to understand a client's technology. In litigation over a machine that has an advanced technological component, for example, the litigator would need to understand how the component operates in order to conduct and respond to discovery regarding that machine. Otherwise, without understanding how the technology and machine work, the lawyer would be incompetent to respond about what is possible to produce.

c. eDiscovery

Attorneys should understand the technological tools available, like eDiscovery, and how to use it to maximize effectiveness and the ability to be the best possible advocate for his or her clients. For example, there are technologies that help assess redundancy, using predictive coding or other analytics, to exclude irrelevant documents in a massive production. The ethical duty of technology competence would require the lawyer to engage these technologies in massive lawsuits, involving large amounts of documents, as opposed to conducting the review without assistance.

d. Contracting Out Technology Competence

Invariably, there will be client matters in which the attorney engaged lacks the relevant technology knowledge. Under these circumstances, the standards of technology competence can be satisfied by hiring trusted third party specialists who can be monitored during the course of the project.

e. Predictive Coding

One circumstance in which technology competence may be outsourced is for the use of predictive coding in discovery. Success with the use of predictive coding hinges entirely on having the experience with and exposure to the complications that may arise so that they may be avoided. Otherwise, the results can be disastrous. Consequently, a component of the ethical duty of technology competence requires the lawyer to ask the right questions of the candidates for the project and to continuously monitor the vendor that is selected to ensure that the most competent specialist handles the work.

f. Cloud Technology

Cloud storage of client information, which generally may implicate an ethical duty for the lawyer or firm to bring in the expertise of a third party in order to determine the security controls and standards used by the cloud storage vendor.

State bar opinions, such as the one decided by the Professional Ethics Committee of the State Bar of Texas, that have provided advice on the ethical obligations arising from use of cloud services, have focused on the questions to ask and the satisfaction lawyers need to obtain from vendors in order to comply with their ethical obligations, such as:

What are the vendor's operating procedures?

How will the lawyer or firm verify that those procedures are actually being followed?

How to decide what types of data can be stored on the cloud and what data lawyers will be forbidden from putting in the cloud?

Who within the firm will have access to the information – just lawyers, people working on particular cases?

How will access to information on the cloud be achieved?

Will there be more secure ports for lawyers and professionals?

Generally, the staff in the law firm's Information Technology Department will have the required insight and background information on which vendors to engage from a security standpoint. Because the ethical duty of technology competence will consider all of the circumstances surrounding a lawyer's decision, opting for a cloud service provider may be the required choice because many cloud storage providers spend heavily on security and offer a more secure environment than what the law firm might already have in place. Given the additional security, it could be less expensive and more reasonable for a law firm to use a cloud vendor than to update its own security measures.

2. Duty to Supervise

ABA Model Rules 5.1[6] and 5.3[7] require lawyers to competently supervise associates, staff and outside services that work with sensitive or confidential information, including personally identifiable information (PII) and personal health information (PHI). These Rules goes hand in hand with compliance under Rule 1.1.

3. Consequences for Failure to Meet Technology Competence Requirements

As demonstrated in *Tellermate*, sanctions are a significant potential consequence if a lawyer is not technologically competent. Of course, another is loss of clients. Clients who are sophisticated in technology reasonably expect that the lawyers engaged will have or hire the expertise to efficiently manage a matter. Otherwise, they will fire the firm.

IV. CONSEQUENCES OF A BREACH: *SHORE V. JOHNSON & BELL*

A mid-size law firm recently discovered the potential consequences of a lax data security measures.[8] Former clients of Johnson & Bell, Ltd., a Chicago law firm, filed a class action against the firm for its allegedly lax security practices and moved for injunctive relief. The plaintiffs exposed purported weaknesses in the firm's web-based time-tracking system, virtual private network, and email system. The

---

[6] *See http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_1_responsibilities_of_a_partner_or_supervisory_lawyer.html.*

[7] *See http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant.html.*

[8] *Shore v. Johnson & Bell, Ltd., No. 1:16-cv-04363, Pacer Doc. 8 (N.D. Ill. Apr. 15, 2016) (Verified Class Action Complaint and Demand for Jury Trial).*

plaintiffs claimed that the corresponding software were outdated, or featured known penetration vulnerabilities, or both. The complaint asserted four causes of action for breach of contract, negligence (legal malpractice), unjust enrichment, and breach of fiduciary duty. The complaint's allegations must have stung especially hard because firm attorneys had, two years earlier, published an article "showcasing" the firm's professed expertise in cyber-security matters.

Significantly, the plaintiffs did not allege that the firm had suffered an actual or attempted breach, or that their confidential information had been stolen and they had suffered an actual tangible injury. They merely alleged, *inter alia*, that "Johnson & Bell [wa]s a data breach waiting to happen."[9] As for injury, the plaintiffs claimed the diminished value of the firm's services and the likelihood of future harm that would result from the theft of their data. Their most tangible loss appears to have been the portion of the professional fees they paid that the firm should have allocated to the "costs of data management and security" and that the firm, allegedly, did not.

The plaintiffs had moved to temporary seal the case when they filed their complaint.[10] They argued that publicizing the details of the firm's system vulnerabilities would place them under "a heightened risk of . . . injuries." The court agreed and granted the motion. The plaintiffs dismissed their claims (without prejudice to proceed in arbitration) after the firm fixed the vulnerabilities, and moved to unseal the case. The court invoked "the presumption of public access" to litigation and, in the absence of a contrary compelling argument by the firm, granted the motion to unseal. The case is now in confidential arbitration per the terms of the firm's engagement letter. But the granted motion to unseal gave the lawsuit the publicity that the firm almost certainly hoped to avoid, whatever the merits of the plaintiffs' allegations.

As noted, the plaintiffs did not allege an actual breach and injury, and the general rule is that tort claims do not stand in the absence of damages. This result does not imply by any means that law firms should not fear potential (as opposed to actual) data breaches. As this next section of the article shows, complaint counsel at the Federal Trade Commission ("FTC") have taken the very aggressive position that lax data security measures are, in and of themselves, violations of Section 5 of the FTC Act, that is, even in the absence of a data breach.

V. GOVERNMENT ENFORCEMENT IN CASE OF BREACH: *IN RE LABMD*

In a unanimous opinion written by Chairwoman Edith Ramirez, the Federal Trade Commission ("FTC") reversed an Administrative Law Judge's ("ALJ") decision that had dismissed Section 5 (15 U.S.C. § 45, the "FTC Act") claims against LabMD for an eight-year-old data breach.[11] The FTC held that the ALJ applied the wrong legal standard and ordered now-inactive LabMD to comply with a number of data-protection measures.[12] The decision is important because it helps set the threshold conditions under which the FTC will consider that a data breach, or *the risk of a data breach*, constitutes a Section 5 violation.

Section 5 of the FTC Act bars "unfair or deceptive acts or practices in or affecting commerce" and authorizes the FTC to police such conduct.[13] But the FTC's authority is restricted to acts that, *inter alia*, cause or are "likely to cause substantial injury to consumers."[14] The FTC has used the FTC Act to police

---

[9] *Id. at 12.*
[10] *Shore v. Johnson & Bell, Ltd., No. 1:16-cv-04363, Pacer Doc. 56 (N.D. Ill. Dec. 8, 2016) (Memorandum Opinion and Order).*
[11] *Opinion of the Commission, In re LabMD, Inc., FTC No. 9357 (July 29, 2016) (hereinafter "Commission Opinion"). The In re LabMD pleadings are available at https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter. See also Pierre Grosdidier, Speculative Data Breach Damages Might Be Actionable, excerpted from State Bar of Texas, Computer and Technology Section's Circuits Newsletter, May 2016, available at http://www.haynesboone.com/news-and-events/news/publications/2016/05/26/speculative-data-breach-damages-might-be-actionable.*
[12] *Final order, In re LabMD, Inc., FTC No. 9357 (July 28, 2016).*
[13] *15 U.S.C. § 45(a)(1)–(2).*
[14] *Id. § 45(n).*

companies whose inadequate or ineffective security measures have resulted in data breaches and, consequently, consumer harm.[15]

The account of the FTC's proceeding against LabMD is convoluted and controversial. LabMD was a medical testing services company that unwittingly granted public access via peer-to-peer software to a large file (the "1718 File") that contained the Personally Identifiable Information ("PII") of some 9,300 patients, including social security numbers and medical data. The FTC filed a complaint against LabMD after Tiversa, Inc., a third-party, found the 1718 File and turned it over to the FTC under contentious circumstances. The ensuing polemic led to a Congressional inquiry and report that cast the FTC and Tiversa in an unflattering light.[16] LabMD eventually unwound its operations in 2014 and the FBI raided Tiversa in March 2016.[17]

The Commission found that the record supported FTC Complaint Counsel's claim that LabMD's data security measures fell substantially short of minimum established norms, especially for a facility that housed medical PII for over 750,000 patients.[18] Unauthorized access protection was very weak and security audits lackadaisical. At least six employees used the password "labmd," for example, and LabMD's IT services failed to detect the peer-to-peer software until the breach occurred. But the record also shows that only Tiversa accessed the 1718 File and no one ever complained, or presented evidence, of a tangible injury because of the data breach.[19]

In its action against LabMD, Complaint Counsel took the position, *inter alia*, that a company's lax computer security measures are actionable under the FTC Act even in the absence of a data breach.[20] According to this argument, Section 5 liability can be imposed merely based on the risk that inadequate security measures will cause a data breach resulting in future consumer harm. In its Initial Decision dismissing the FTC's complaint, the Administrative Law Judge ("ALJ") specifically rejected this argument because it required too many speculative steps between the lax security and actual consumer harm.[21] In dismissing Complaint Counsel's claim regarding the 1718 File, the ALJ also held that "Complaint Counsel ha[d] proven the 'possibility' of harm, but not any 'probability' or likelihood of harm."[22]

In reversing the ALJ, the Commission held that the release of the 1718 File, which contained sensitive personal medical information, caused sufficient consumer injury to satisfy the Section 5 threshold.[23] This was so even though only Tiversa accessed the 1718 File. The Commission also held separately that the exposure of the 1718 File for 11 months on a peer-to-peer file-sharing site was in and of itself actionable under Section 5 because it created a "significant risk" of substantial consumer injury.[24] The unauthorized release of one file containing PII to one party is, therefore, actionable under Section 5, as is publicly exposing such a file through peer-to-peer software even in the absence of evidence of actual copying.

---

[15] *Commission Opinion at 10 n.21 ("[t]o date, using both its deception and unfairness authority, the Commission has brought nearly 60 data security cases.").*
[16] *Tiversa, Inc.: White Knight or Hi-Tech Protection Racket?, Comm. on Oversight and Gov't Reform, U.S. House of Rep., 113th Cong. (Jan. 2, 2015) ("Committee Report").*
[17] *http://www.theregister.co.uk/2016/03/18/fbi_raids_cybersecurity_firm_tiversa/.*
[18] *Commission Opinion at 11–16.*
[19] *Tiversa also shared the 1718 File with an academic researcher.*
[20] *Complaint Counsel's Appeal Brief, In re LabMD, Inc., FTC No. 9357, at 5–7, 10–12 (Dec. 22, 2015).*
[21] *Initial Decision, In re LabMD, Inc., FTC No. 9357, at 84–85 (Nov. 13, 2015).*
[22] *Initial Decision at 14.*
[23] *Commission Opinion at 17–19.*
[24] *Id. at 20–25.*

But, significantly, the Commission expressly declined to address Complaint Counsel's "broader argument" that inadequate security measures that potentially expose PII to a breach constitute a Section 5 violation in and of themselves:

> We note that Complaint Counsel argues that LabMD's security practices risked exposing the sensitive information of all 750,000 consumers whose information is stored on its computer network and therefore that they create liability even apart from the LimeWire incident. We find that the exposure of sensitive medical and personal information via a peer-to-peer file-sharing application was likely to cause substantial injury and that the disclosure of sensitive medical information did cause substantial injury. Therefore, we need not address Complaint Counsel's broader argument.[25]

The Commission, therefore, saw no need to opine on Complaint Counsel's most reaching argument. Companies that host large quantities of PII would be ill-advised to find solace in the Commission's restraint given the zeal that the FTC showed in policing the LabMD breach, however. This is especially so since hacker's ever-growing sophistication arguably constantly shift what constitutes a "significant risk" of data breach and, therefore, consumer injury. Meanwhile the controversy continues: LabMD has already stated its intent to appeal the Commission's decision to a Court of Appeals.[26]

VI. WHAT CAN A FIRM DO?

Cyber-security breaches and data leaks continue to be matters of serious concern to companies and consumers alike. Verizon reported 3,141 data disclosures in 2015, up from 2,122 in 2014.[27] In 2015, Americans reported 490,220 incidents of identity theft, defined as the use or attempted use of another's sensitive Personally Identifiable Information ("PII") to commit fraud.[28] PII consists of, *inter alia*, a person's name, address, date of birth, Social Security number, driver's license number, credit card and bank account numbers, phone number, and biometric data.[29]

The Federal Trade Commission Act, 15 U.S.C. §§ 41 *et seq*., grants the FTC the authority to regulate cyber-security, including the right to bring administrative enforcement actions against companies with unreasonable data security practices. Circuit and district court rulings affirming the Commission's jurisdiction over cyber-security practices have bolstered this authority.[30] In 2015 the Third Circuit ruled that the FTC Act grants the Commission authority to challenge "unfair" data security practices.[31] The Commission has aggressively exercised this authority and has brought close to sixty enforcement actions to date.[32]

Other agencies are also concerned with the handling of consumer information—the Department of Health and Human Services' ("HHS") Health Insurance Portability and Accountability Act (HIPAA) sets

---

[25] *Id. at 16.*
[26] *Allison Grande, FTC Revives LabMD Data Leak Suit, Finds Consumer Harm, Law360 (July 29, 2016).*
[27] *Verizon, 2016 Data Breach Investigations Report 1 (2016); 2015 Data Breach Investigations Report 1 (2015).*
[28] *Verizon, 2016 Data Breach Investigations Report 1, supra note 1; Federal Trade Comm'n, Guide for Assisting Identity Theft Victims 4, (2013).*
[29] *Guide for Assisting Identity Theft Victims 4, supra note 2.*
[30] *Allison Grande, LabMD Ruling Puts FTC in Driver's Seat on Data Security, LAW360 (May 13, 2014, 8:41 PM); Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 246–48 (3d Cir. 2015).*
[31] *FTC v. Wyndham Worldwide Corp., 799 F.3d at 248, 259.*
[32] *Opinion of the Commission at 10, n.21, In the Matter of LabMD, Docket No. 9357 ("To date, using both its deception and unfairness authority, the Commission has brought nearly 60 data security cases."); Fed. Trade Comm'n, Commission Statement Marking the FTC's 50th Data Security Settlement 1 (2014); Leslie Fair, FED. TRADE COMM'N, Start with Security: New Guide Offers Lessons from FTC Cases (June 30, 2015, 12:00 PM).*

standards for the protection of medical records and personal health information.[33] HHS's Office of Civil Rights enforces the HIPAA Privacy and Security Rules.[34] The Securities and Exchange Commission may also soon be involved in data security requirements. Senators Jack Reed (D-RI) and Susan Collins (R-ME) have proposed a bill that would direct the SEC to adopt rules requiring a company to disclose whether it has a cyber-security expert on its board and other measures in place to prevent a data breach.[35]

Given the recent Third Circuit ruling and the FTC's position of authority, and in light of other federal agencies' increasing attention to cyber-security, businesses should be interested in not only how to prevent a data breach, but also how to avoid a government investigation. This article focuses on the FTC's 2015 guidelines for data security.

A. Ambiguities in Data Security Standards and Liability

The lack of clear-cut rules for data security practices has the potential to create ambiguities.[36] The FTC issues complaints against companies for "unfair" data security practices, but what constitutes an "unfair" practice in this area is not clearly defined.[37] Rather, the FTC decides this issue on a case-by-case basis, using a three-part test outlined in Section 5(n) of the FTC Act.[38] An act or practice may be deemed unfair if (1) it "causes or is likely to cause substantial injury to consumers"; (2) the injury "is not reasonably avoidable by consumers themselves"; and (3) the injury is "not outweighed by countervailing benefits to consumers or to competition."[39] It is not clear how this language translates into tangible data security guidelines.

In the recent controversial case of *In re LabMD*, discussed above, the FTC's Complaint Counsel alleged, *inter alia*, that the mere act of maintaining inadequate security measures on a computer that hosts protected data is enough to breach the FTC Act. Under this test, proof of actual data release identity theft would not be required for liability.[40] Like Wyndham before it, LabMD argued that the FTC Act did not provide fair notice of the conduct required.[41] Wyndham, a hotel chain, was hacked three times in a row, resulting in the theft of 619,000 consumer payment card account numbers and $10.6 million in fraudulent charges.[42] In *FTC v. Wyndham Worldwide Corp*., the Third Circuit Court of Appeals found that Wyndham had fair notice of the standards for data security. However, Wyndham focused its lack of fair notice argument on "the FTC's failure to give notice of its interpretation of the statute" and did not "meaningfully argue that the statute itself fails fair notice principles."[43] The court also stated that respondents are entitled to a low level of statutory notice because Section 45(a) does not implicate any constitutional rights.[44] Wyndham had fair notice as long as it could "reasonably foresee that a court could construe its conduct as falling within the meaning of the statute."[45] The court also mentioned that Wyndham failed to follow the

---

[33] *U.S. DEP'T OF HEALTH & HUMAN SERVS., The HIPAA Privacy Rule (last visited Sept. 9, 2016); U.S. DEP'T OF HEALTH & HUMAN SERVS., The Security Rule (last visited Sept. 9, 2016).*
[34] *U.S. DEP'T OF HEALTH & HUMAN SERVS., HIPAA Enforcement (last visited Sept. 9, 2016).*
[35] *Ted Trautmann, Call to Action: Planning for the Inevitable Cyberattack, 19 SEC TODAY 1, 1 (2016). Text of Senate Bill S.2410 available here: https://www.congress.gov/bill/114th-congress/senate-bill/2410/text.*
[36] *Allison Grande, FTC Resolute on Data Security Despite Wyndham Fight, LAW360 (Sept. 9, 2013, 8:37 PM); Elliot Golding, FTC Data Security Authority Remains Murky Despite Wyndham, LAW360 (April 8, 2014, 2:44 PM).*
[37] *15 U.S.C.A. § 45.*
[38] *Golding, supra note 10; FED. TRADE COMM'N, START WITH SECURITY 1 (2015).*
[39] *15 U.S.C. § 45(n).*
[40] *Complaint Counsel Corrected Appeal Brief at ii, In the Matter of LabMD, Inc., 2016 FTC LEXIS 19, No. 9357.*
[41] *LabMD's First Amended Answer and Defenses to Administrative Complaint at 6, In the Matter of LabMD, 2015 FTC LEXIS 184, 8-9; Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 254 (3d Cir. 2015).*
[42] *District Court Opinion at 4–5, Fed. Trade Comm'n. v. Wyndham Worldwide Corp., 10 F.Supp.3d 602, 609, No. 13-1887(ES) (D. N.J. 2014).*
[43] *FTC v. Wyndham Worldwide Corp., 799 F.3d at 255–58.*
[44] *Id. at 255.*
[45] *Id. at 256.*

practices recommended by a 2007 FTC guidebook for businesses, supporting the conclusion that Wyndham had fair notice.[46]

Wyndham was required to implement a series of security measures detailed by the FTC as part of its settlement terms. Some observers saw this as a step in the right direction in laying out "reasonable" data security practices with more specificity.[47] Because the majority of the FTC's enforcement actions in the data security area are resolved through settlement and consent orders, the FTC has referred to these results as a kind of "common law light" that should inform other companies' practices.[48]

B. 2015 FTC Guidelines

Perhaps in response to complaints regarding the ambiguities of data security standards, in June 2015 the FTC published a set of guidelines for businesses dealing in sensitive consumer information.[49] These guidelines draw from recent FTC settlements and recommend certain policies based on other companies' errors or deficient security practices.

These are not hard-and-fast rules—the FTC recognizes that security practices vary; what is appropriate for a multi-million dollar company handling complex transactions may not be appropriate for a mom-and-pop shop. "The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[50] In *LabMD*, the FTC pointed out that "as the Commission has stated in this case, a company that has maintained reasonable security would not be liable under Section 5 merely because a breach occurred."[51]

The FTC's guidelines offer the following advice:

- **Do not collect unneeded information**. Hold onto needed information only as long as a legitimate business need exists. LabMD allegedly maintained the personal information of 1,000,000 consumers, for some of whom the company never performed any tests.[52] This practice became part of the basis of the FTC's complaint against LabMD.

- **Restrict access to data.** Twitter provoked an FTC investigation and complaint by allowing almost all employees, regardless of their job duties, to view users' nonpublic tweets and other information and to send tweets on behalf of users.[53]

- **Require secure passwords**. "Qwerty" and "121212" are no better than having no password at all. The Commission was also quick to point out that "at least six employees used 'labmd' as their login password" in its *LabMD* opinion.[54]

- **Suspend or disable users after a certain number of unsuccessful login attempts.** Like the

---

[46] *Id. at 257.*
[47] *Allison Grande, FTC Tips Data Security Hand in Wyndham Pact, LAW360 (Dec. 10, 2015, 10:21 PM).*
[48] *Julie Brill, Commissioner, Federal Trade Comm'n, Privacy, Consumer Protection, and Competition 2–3, Loyola University Chicago School of Law, 12th Annual Antitrust Colloquium (April 27, 2012).*
[49] *Fed. Trade Comm'n, Start with Security 1.*
[50] *Commission Statement Marking the FTC's 50th Data Security Settlement 1, supra note 4.*
[51] *FTC Reply Brief at 16, In the Matter of LabMD, Inc., (citing Order Denying Respondent's Motion to Dismiss at 18 (". . . the mere fact that such breaches occurred, standing alone, would not necessarily establish that LabMD engaged in 'unfair . . . acts or practices.")).*
[52] *Complaint at 2, In the Matter of LabMD, Inc.; Complaint Counsel Corrected Appeal Brief at 4, 2016 FTC LEXIS 19, 4.*
[53] *Complaint at 2, In the Matter of LabMD, Inc.*
[54] *Opinion of the Commission at 2, In the Matter of LabMD, Docket No. 9357.*

monkeys left alone in a room with a typewriter who will eventually type out all of Shakespeare's plays, hackers use a method that types endless combinations of characters until they luck into the right one. Ten successive failed logins should hint that something nefarious is afoot.

- **Store and transmit sensitive information securely.** Train personnel and use accepted encryption methods—no need to reinvent the wheel. ValueClick, Inc.'s use of a proprietary, nonstandard, and untested form of encryption brought on an FTC complaint and subsequent $2.9 million settlement.[55]

- **Segment networks and monitor who is trying to get in and out.** The FTC brought a complaint against DSW, Inc. for failing to limit computers on one in-store network from connecting to computers on other in-store and corporate networks, making it possible for hackers to use one network to connect to other networks.

- **Secure remote network access.** The FTC brought a complaint against Lifelock, Inc. a company marketing identity theft prevention services, for allegedly failing to require antivirus programs on computers used for remote access to its network.[56] Similarly, mortgage lender Premier Capital Lending, Inc. attracted the FTC's attention by activating a remote login account for a business client without assessing the client's security, allowing hackers to access the client's system and steal remote login credentials and consumer information.

- **Apply security practices when developing new products or services.** Verify that privacy and security features actually work—test that a photograph will "disappear forever" before promising to consumers that it will.[57]

- **Verify that third-party service providers also use appropriate security measures.** The FTC recommends that businesses insert security standards into their contracts and ensure their partners' compliance.

- **Implement software updates regularly and develop a process to receive and address reports of vulnerabilities.** Another of the FTC's allegations against Lifelock was that it failed to install critical network updates, leaving its network vulnerable to unauthorized access.[58]

- **Do not leave sensitive information out in the open or toss it in the dumpster.**[59] When disposing of equipment or paperwork, devices should be wiped clean and documents should be shredded or burned. The FTC has brought complaints against companies for storing paperwork with sensitive information in boxes in a garage; leaving a laptop with sensitive information in a locked car; tossing paperwork in a dumpster; and selling hard drives without first clearing them.

By and large, it appears that FTC investigations are not triggered by one minor misstep, but by a fundamental failure to implement reasonable procedures to protect sensitive information. Records of FTC complaints and settlements can be found on the FTC's website. The guidelines are available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

These guidelines are a high-level checklist that IT experts may find simplistic or overly general. But this list is a good starting point for a dialog between in-house counsel and IT professionals about the state

---

[55] *Press Release, Federal Trade Commission, ValueClick to Pay $2.9 Million to Settle FTC Charges (March 17, 2008).*
[56] *Complaint at 10, FTC v. LifeLock, Inc., No. 2:10-cv-00530-MHM (FTC 2010).*
[57] *Complaint at 2–3, In the Matter of Snapchat, Inc., No. C-4501 (FTC 2014).*
[58] *Complaint at 10, FTC v. LifeLock, Inc.*
[59] *Press Release, Federal Trade Commission, CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations (Feb. 18, 2009).*

of data security within a company. The guidelines are also written simply enough for a lay person to understand and then go to the IT professional with questions about what kind of data protection exists and what improvements are necessary in the future to meet the FTC's expectations.

C. The American Corporate Counsel's Model Information Protection and Security Controls for Outside Counsel

Although the controls in the ACC's Guidelines for outside counsel's information protection and security are written to resemble model contract clauses, they merely establish a starting point as opposed to a standard that must be observed. Not all of the guidelines will apply to every law firm. While certain measures may be too burdensome under the circumstances, they include a number of measures firms will need to consider carefully. They are intended to start a conversation that should be had between all sizes of law firms and their clients. The Guidelines address a broad range of data-security-related measures including: data breach reporting, data handling and encryption, physical security, employee background screening, information retention/return/destruction, and cyber liability insurance.[60]

[60] *See https://www.acc.com/advocacy/upload/Model-Information-Protection-and-Security-Controls-for-Outside-Counsel-Jan2017.pdf?_ga=1.82398227.488119238.1490817924.*