Protection of Client Confidential Information from Cyberattacks Is a Compelling Business and Ethical Priority for Inside and Outside Corporate Counsel

*By E. Norman Veasey**

Criminal cyberattacks are rampant. The criminals who launch these attacks target law firms and businesses mercilessly—around the clock. Inside and external corporate counsel have an urgent responsibility not only to understand the perils that these attacks present to law firms and corporate law departments but also to take defensive action.

This article briefly mentions some of the criminal tactics that have resulted in horror stories of cyberattacks. The principal mission of the article, however, is not to expound on technological issues but rather to highlight the ethical responsibility of individual lawyers and firm leaders in protecting client information.

Many cyberattacks should be preventable with an understanding of vulnerable areas, attack methods, and the preventive steps that lawyers and firms should undertake. Inside corporate counsel and external lawyers cannot be expected to be technological experts. Rather, individual lawyers and law-firm managers need to realize the nature and extent of the peril and see to it that preventive measures are implemented with expert assistance.

Central to this article is an analysis of the American Bar Association's ("ABA's") Model Rules of Professional Conduct ("Model Rules") and its Official Comments on protecting client information. The Model Rules have been amended to emphasize that lawyers must keep abreast of the benefits and risks associated with relevant technology, and that lawyers must make reasonable efforts to prevent unauthorized access to client information. A substantial majority of jurisdictions, but not all jurisdictions, have adopted these amendments. This article urges the remaining jurisdictions to follow that lead.

"[L]aw firms around the world: you are and will be targets of cyber hacking, because you have information valuable to would-be criminals."[1]

* E. Norman Veasey is a member of the Delaware Bar and former Chief Justice of the Supreme Court of Delaware (1992–2004), and he is currently Special Counsel to the Wilmington, Delaware, firm of Gordon, Fournaris & Mammarella, P.A. ("GFM"). The author is extremely grateful to the Honorable Collins J. Seitz, Jr. (Justice of the Supreme Court of Delaware), Barbara S. Gillers, Esquire, of the New York Bar, Lucian T. Pera, Esquire, of the Tennessee Bar, Charles Slanina, Esquire, of the Delaware Bar, and Kate Mahoney, Esquire, of the Delaware Bar for their valuable counsel and critique in reviewing and commenting on an earlier draft of this article.

1. U.S. Attorney's Office S. Dist. of N.Y., *U.S. Attorney Announces Arrest of Macau Resident and Unsealing of Charges Against Three Individuals for Insider Trading Based on Information Hacked from Prominent U.S. Law Firms*, U.S. DEP'T JUST. (Dec. 27, 2016), https://www.justice.gov/usao-sdny/pr/manhattan-us-

Introduction and Scope

This article is a renewal of wake-up calls for individual lawyers and those in leadership positions in law firms and corporate law departments to keep abreast of the benefits and risks of changes in technology and take reasonable steps to prevent cybercrime attacks that threaten to compromise confidential client information. Of course, this is not the first such clarion call. Not only do individual lawyers have a responsibility to understand the benefits and risks of technology and make reasonable efforts to prevent a compromise of client information, managers in each law firm and corporate law department must exercise supervisory responsibility to ensure firm-wide compliance with ethical standards.

Law firms, corporate law departments, banks, and other businesses have become sitting ducks for exploitation by cybercriminals. Not only are these entities themselves the potential victims of the bad guys, their clients and their counterparties are the principal targets (and sometimes even more so). And when client information is compromised by cyberattacks that lawyers could have prevented by using the right safeguards, and a data breach results, it is the lawyer and the lawyer's firm management that will likely take the fall.

This article is not a technological primer on technology. Indeed, the author does not presume to have the expertise to opine on technological matters. The sole mission of this article is to remind lawyers and those in firm management of their professional responsibilities of awareness, action, and compliance. It narrowly focuses on three principal objectives: (1) to engender a critical awareness of cyber threats in individual lawyers; (2) to emphasize ethical supervisory responsibilities to the hierarchy of corporate law departments and outside-counsel firms; and (3) to urge universal jurisdictional adoption of the modern Model Rules and their Official Comments in this area.

Some Horror Stories

There are many horror stories dramatizing how law firms, businesses, and governments have been victimized by the various cyber weapons that the "bad guys" deploy—in fact, there are so many illegal schemes afoot that listing them all would fill this entire issue.[2] There are also many types of cyber criminals, and they have varying motives. Some may be young, fun-seeking, annoying hackers. Others may be serious criminals bent on malicious electronic disabling (sometimes for ransom), espionage, or profiteering. The profiteering cybercrime category includes those who seek to penetrate a law firm's computer system to steal valuable information, including that of its clients.

attorney-announces-arrest-macau-resident-and-unsealing-charges-against (quoting Preet Bharara). Bharara was the U.S. Attorney for the Southern District of New York from 2009–17.

2. *See The Most Common Social Engineering Acts*, Infosec (Feb. 6, 2019), https://resources.infosecinstitute.com/common-social-engineering-attacks/#gref (providing a recent summary of cyberattack schemes).

This article focuses exclusively on the ethical responsibilities of lawyers to protect client information. Nevertheless, the general and pervasive impact of cybercrime goes well beyond the scope of this article. For example, in July 2019, Capital One—a large bank—was hit by cybercriminals, causing a massive data breach. A report in *The New York Times* on July 31, 2019, noted the scope of such attacks and emphasized that hackers need only find one weak spot, whereas the potential targets must mount an all-encompassing defense:

> Large financial companies have to thwart hundreds of thousands of cyberattacks every single day. Data thieves have to get lucky only once.
>
> Big banks like Capital One, the victim of a recent attack that captured the personal information of over 100 million people, are a target for digital troublemakers, like individual hackers trying to impress their peers or intelligence operatives for foreign governments.
>
> A single weak spot is all savvy hackers need. And they often find them. Already this year, there have been 3,494 successful cyberattacks against financial institutions, according to reports filed with the Treasury Department's Financial Crimes Enforcement Network.[3]

As for the lawyer-ethics focus of this article, the following is a reference to only a very few examples of some horror stories.

Cybercrime has evolved beyond traditional hacking to include sophisticated social-engineering scams that rely on the errors of unwitting insiders to effectuate the criminals' schemes. Criminals use trickery to outwit their victims, often creating a sense of urgency combined with fear. In the past several years, organizations around the world have been the victims of multimillion-dollar fraud schemes that were successfully perpetrated online using social engineering.[4] The term "social engineering" has become common in the context of information security, depicting the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.[5]

One frequent category of social engineering attacks includes "phishing" or "spear phishing." Both types are usually implemented by sending an innocuous-looking email to an employee of a law firm or other business inviting the recipient to open an attachment or link, thereby introducing malware into the firm's

3. Stacy Cowley & Nicole Perlroth, *One Gap in Bank's Armor, and a Hacker Slips In*, N.Y. Times, July 31, 2019, at 1. Of course, cyberattacks by Russia and others against the United States on an international scale are a significant and escalating national-security problem that cries out for deterrents and defenses. *See, e.g.*, Susan Hennessey, *Deterring Cyberattacks, How to Reduce Vulnerability*, Foreign Affairs, Nov./Dec. 2017, at 39.

4. There is excellent information on these issues in one of the most comprehensive and helpful sources available: *The ABA Cybersecurity Handbook* ("*Cybersecurity Handbook*"). *See* The ABA Cybersecurity Handbook (Jill D. Rhodes & Robert S. Litt eds., 2d ed. 2018). The *Cybersecurity Handbook* is referred to throughout this article.

5. *Social Engineering*, Lexico, www.lexico.com/en/definition/social_engineering (last visited Oct. 20, 2019).

system. The common scheme of phishing can be an untargeted mass scam. Spear phishing, however, is carefully tailored to attack a specific target.

> *Phishing Attacks*. Phishing is among the attack vectors used most often by hackers to launch cyber attacks. The main perpetrators of phishing attacks are organized crime syndicates and state-affiliated actors. "The most devastating attacks by the most sophisticated attackers almost always begin with the simple act of spear-phishing," then-Homeland Security Secretary Jeh Johnson observed at the November 2016 Financial Crimes and Cybersecurity Symposium hosted by the Manhattan District Attorney's office. *Phishing* has been a long-standing cyber threat for law firms.[6]

For example, several years ago three Toronto law firms were victimized through targeted "phishing attacks," later found to have come from criminals in China. In one of those cases, a law-firm bookkeeper unwittingly clicked on a malicious email attachment, which set up a "Trojan banker" virus,[7] thus establishing a "backdoor" to the firm's electronic files through the bookkeeper's computer. Once the backdoor to the firm's files was opened, the criminals were able to mimic a bank's website to lure unsuspecting users into entering their critical information. The criminally introduced viral program then transmitted the information to the hackers, who were able to monitor and divert deposits, thus enabling them to steal a significant amount of money.[8]

Trojan banker scams derived from phishing are one example, but there are many other types of scams. For example, one scam sometimes known as "Business E-Mail Compromise" ("BEC") has targeted many businesses (including law firms) by compromising legitimate email accounts through social engineering or computer-intrusion techniques to divert funds (such as real-estate settlement funds) from their intended destinations to unauthorized accounts controlled by the criminals. There have been victims of BEC scams in all fifty states and across 150 countries.[9]

Another example involves insider-trading schemes. In one set of cases, three Chinese nationals hacked into prominent international law firms in New York City and penetrated the email accounts of partners who were negotiating high-profile merger-and-acquisition ("M&A") transactions with lawyers for their counterparties. According to an indictment and a U.S. Securities & Exchange Commission ("SEC") civil case, the hackers stole a law-firm employee's log-in credentials to access each firm's email server and then plant malware.[10] Once they had access to the law firms' servers, the criminals were able to log in to email accounts of the specific partners at the firms who were negotiating the M&A transactions with lawyers for the counterparties.

Once they logged in, the criminals were able to learn details of the merger negotiations, including pricing information. They then traded on the surreptitiously

6. Lucy L. Thomson, *Understanding Cybersecurity Risks*, *in* THE ABA CYBERSECURITY HANDBOOK, *supra* note 4, at 11, 22.
7. *Id.* at 22.
8. *Id.* at 23.
9. *Id.* at 28.
10. *See* U.S. Attorney's Office S. Dist. of N.Y., *supra* note 1.

obtained, nonpublic pricing information before the deals were made public. In one series of transactions detailed in SEC filings, the hackers made multimillion-dollar insider-trading profits.[11] In 2016, Bharara made the following statement about one of the cases and the vulnerability of law firms:

> This case [(*United States v. Iat Hong*)] of cyber meets securities fraud should serve as a *wake-up call for law firms* around the world: you are and will be targets of cyber hacking, because you have information valuable to would-be criminals.[12]

Observations about these vulnerabilities and schemes abound because law firms are such tempting targets for cyberattacks:

> Throughout the course of representing clients, lawyers receive volumes of sensitive and confidential data and information—attorney-client privileged information, client trade secrets, and all types of personally identifiable information (PII), financial, healthcare, law enforcement, and many other types of records.
>
> * * *
>
> In addition, law firms acquire a staggering array of sensitive information in e-discovery. It is a sobering fact that much of the data and information obtained by law practices may have been created, used, and maintained in a secure environment, and then transferred, often without the knowledge, agreement, or consent of the individual or organization that created or collected the information, to an environment where the extent of security protections may be unknown or is not assured.
>
> To protect confidential information, lawyers and law firms must know what data they have, where it resides, its level of sensitivity, and how it is secured. In addition to the more obvious places for data such as computer servers, desktop and laptop computers, and mobile devices, information may reside in other, somewhat less expected locations. For example, back-ups can contain significant amounts of sensitive information. Also, sensitive data may be downloaded from e-mail onto a mobile device and then saved locally. These devices are likely to be linked to the user, not the law firm, which means that the sensitive data is then backed up to the user's personal cloud account, completely outside law firm control.[13]

That law firms have access to staggering amounts of confidential or otherwise sensitive information is not exactly breaking news, and these types of cybercrimes are not new events. But these pernicious crimes have proliferated,[14]

11. *Id.*

12. Thomson, *supra* note 6, at 11 (emphasis added); *see* United States v. Hong, C.A. No. 16-cv-9947 (S.D.N.Y. Dec. 27, 2016); U.S. Secs. & Exch. Comm'n, Litigation Release No. 23711 (Dec. 27, 2016), https://www.sec.gov/litigation/litreleases/2016/lr23711.htm; *see also* U.S. Attorney's Office S. Dist. of N.Y., *supra* note 1.

13. Thomson, *supra* note 6, at 16.

14. *See, e.g.*, Comm. on Commerce, Sci. & Transp., Business Cyber Risk, Cybersecurity for Your Law Firm (2016); Comm. on Commerce, Sci. & Transp., A "Kill Chain" Analysis of the 2013 Target Data Breach (Mar. 26, 2014); Benjamin Dynkin & Barry Dynkin, *Anatomy of a Cyber Attack*, Law.com: N.Y.L.J. (Apr. 4, 2018, 2:35 PM); Maria Korolov & Lysa Myers, *What Is the Cyber Kill Chain? Why It's Not Always the Right Approach to Cyber Attacks*, CSO (Nov. 7, 2017, 9:40 PM),

thus increasing client awareness and the interest of state and federal regulators charged with the responsibilities of enforcing numerous state and federal laws that are designed to control cybercrime and deal with data breaches.[15]

Many managers in corporate law departments and external law firms are hiring experts, establishing security plans, and requiring compliance with defensive measures. Boards of directors and senior officers of corporations are continually ratcheting up their structures and training regimes to elevate awareness, knowledge, and the implementation of crucial, state-of-the-art preventive methods.[16]

The Risk Oversight Advisory Council of the National Association of Corporate Directors ("NACD"), referring to data from the 2018–19 NACD Public Company Governance Survey, recently published a report citing cybersecurity oversight at the top of boardroom priorities. Among many important analyses in this report, it emphasizes that, at "its core, cybersecurity is a people issue, and boards should tailor their oversight accordingly."[17] The same priorities apply to lawyers and law-firm management.

As noted, the thrust of this article is not that lawyers and those in firm management must become technological experts. It is to remind lawyers and law-firm managers that they must be aware of the threats, seek the professional help of experts, take preventive steps, and be adequately covered by cyber-insurance. Most state ethics rules help crystallize these obligations.[18]

https://www.cso.com.au/article/629681/what-cyber-kill-chain-why-it-always-right-approach-cyber-attacks; Charles Slanina, *Cyber Risks*, 42 J. Del. St. B. 16 (May 2019); Julie Sobowale, *6 Major Law Firm Hacks in Recent History*, A.B.A. J. (Mar. 1, 2017, 11:54 AM), http://www.abajournal.com/magazine/article/law_firm_hacking_history; Phyllis Sumner, *Notes from a Law Firm Chief Privacy Officer: New Demands*, Law360 (Aug. 14, 2017, 1:13 PM), https://www.law360.com/articles/952911/notes-from-a-law-firm-chief-privacy-officer-new-demands; Verizon, 2019 Data Breach Investigations Report (2019), https://enterprise.verizon.com/en-gb/resources/reports/dbir/2019; *U.K. Regulator Announces Hefty GDPR Fines for Cybersecurity Failures*, Wachtell, Lipton, Rosen & Katz (July 10, 2019).

15. *See, e.g.*, John Bandler, Cybersecurity for the Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security 313–14 (2017); Delaware Data Protection Statute, Del. Code Ann. tit. 6, § 12B-100 *et seq.*; Dustin Volz & Byron Tau, *FBI Retooling Once Again Sets Sights on Expanding Cyber Threats*, Wall St. J., Mar. 29, 2019, at 1; David Zetoony, *Data Privacy and Security: A Practical Guide for In-House Counsel*, 77 Wash. L. Found. Contemporary Legal Notes (May 2016), https://iapp.org/media/pdf/resource_center/WLFDataPrivacyandSecurityHandbook.pdf. For an excellent list of selected statutes, regulations, and cases, see The ABA Cybersecurity Handbook, *supra* note 4, at 341–68 (providing the appendices to Chapter 4).

16. *See* Angeline G. Chen, *In–House Counsel*, *in* The ABA Cybersecurity Handbook, *supra* note 4, at 219.

17. Nat'l Ass'n of Corp. Directors Risk Oversight Advisory Council, Current and Emerging Practices in Cyber-Risk Oversight (2019).

18. As noted throughout, I have made extensive references to the *Cybersecurity Handbook*. It is an important document that is chock full of articles and appendices analyzing these issues and providing numerous sources. The appendices to the *Cybersecurity Handbook* include the text of selected security statutes, regulations, and cases (pp. 341–68) as well as ABA and state bar association ethics opinions and other resources regarding lawyers' ethical obligations to provide data security to their clients (pp. 369–430). Likewise, the appendices contain an excellent reference to incident response and cyber insurance coverage on pp. 431–45.

Overview of Applicable Model Rule Provisions[19]

The ABA's last major revision of the Model Rules was concluded in 2002, with the adoption by the ABA House of Delegates of comprehensive, then-modern revisions. Those revisions were based in large part on the recommendations of the ABA Commission on Evaluation of the Rules of Professional Conduct ("Ethics 2000 Commission").[20] As with all societal developments, times change.

Since the early days of the twenty-first century, communications and commerce have become increasingly globalized and technology based. Lawyers have facilitated many of these changes. Globalization and technology-intensive changes, therefore, have necessitated a comprehensive study of technology's impact on law practice. Technology increasingly affects nearly every aspect of legal work, including how lawyers store confidential information, communicate externally with clients and counterparties as well as internally among law firm colleagues, conduct discovery, engage in research, and market their legal services.

In view of this sea change in law practice, the ABA created the Ethics 20/20 Commission. The resulting Ethics 20/20 Commission Report, issued in 2012, recognizes that technology and globalization have transformed the practice of law in ways that the profession could not have anticipated in 2002 when the ABA House of Delegates adopted the Ethics 2000 Commission's changes to the Model Rules.

The Report of the ABA Commission on Ethics 20/20 ("Ethics 20/20 Commission Report") concluded that a lawyer's ethical duty of competence requires that lawyers stay abreast not only of changes in the law but also in the practice of law itself, including the need to understand technology's benefits and risks. Most importantly, the Ethics 20/20 Commission Report advocates a strong ethical requirement that lawyers *shall* undertake reasonable efforts to protect client information.[21]

Resulting Model Rules of Professional Conduct and Official Comments

Following the release of the Ethics 20/20 Commission Report in 2012, the ABA House of Delegates adopted revisions to the Model Rules and Official Comments. Although there were a number of changes to the Model Rules resulting from the Ethics 20/20 Commission Report, the focus of this article is on the changes relating to the professional responsibilities of the individual lawyer and her firm to modernize her competency and to make reasonable efforts to protect client information.

19. The following discussion is based on the Ethics 20/20 Commission Report. *See* Report of the ABA Commission on Ethics 20/20 (2012), https://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105a_filed_may_2012.pdf.

20. The author had the honor of chairing the Ethics 2000 Commission. The Commission's work began in 1997. Through research, public hearings, internal debates, and drafting, the Commission's initial report—in which the Model Rules were significantly revamped—was drafted. It was then presented to the ABA House of Delegates beginning in the fall of 2000. The report was debated, scrutinized, critiqued, amended, and voted upon over a two-year period in a series of House of Delegates meetings, culminating in overall approval in 2002. Over the years thereafter, there have been further amendments to the Model Rules. Most jurisdictions have adopted the bulk of the Model Rules.

21. *See supra* note 15.

The Model Rules and Official Comments that are a focus of this article are (a) the Official Comment to Model Rule 1.1 on competence, and (b) the addition of Model Rule 1.6(c) on information protection. These changes not only apply to individual lawyers but also implicate the supervisory responsibilities of law-firm management pursuant to Model Rule 5.1 and Model Rule 5.3. I have set forth below and in later pages[22] the applicable texts of the Model Rules and Official Comments.[23]

Rule 1.1. Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.[24]

Official Comment

[8] *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.[25]

Rule 1.6. Confidentiality of Information

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by paragraph (b).[26]

* * *

(c) *A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.*[27]

Official Comment

Acting Competently to Preserve Confidentiality

[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client

22. For a discussion of Model Rules 5.1 and 5.3 concerning law-firm management responsibilities, see *infra* at pp. 35–46.

23. The key 2012 changes are highlighted in italics.

24. Model Rules Prof'l Conduct r. 1.1 (Am. B. Ass'n 2018) [hereinafter Model Rules].

25. *Id.* r. 1.1 cmt. [8] (emphasis added).

26. There are seven unrelated existing exceptions in Model Rule 1.6(b). Generally, they permit the lawyer to reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary for the prevention of death, bodily harm, or injury to financial interests, as well as to secure legal advice for the lawyer, establish a claim or defense in a controversy with the client, comply with law or court orders, and resolve conflicts when the lawyer is changing jobs.

27. Model Rule 1.6 (emphasis added).

does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. *Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients* (e.g., *by making a device or important piece of software excessively difficult to use*). *A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule.* Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. *For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]–[4].*

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule [e.g., encryption] or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

[20] *Former client*. The duty of confidentiality continues after the client–lawyer relationship has terminated. See Rule 1.9 (c)(2). See Rule 1.9(c)(1) for the prohibition against using such information to the disadvantage of the former client.[28]

Scope of Client Information Protected by Model Rule 1.6

"Information relating to the representation of a client," referred to in Model Rule 1.6, is a broad phrase that prohibits revealing—unwittingly or otherwise—virtually all information relating to the representation, including confidential

28. *Id.* r. 1.6 cmts. [18–20] (emphasis added). In the case of a former client under Model Rule 1.9(c)(1), the information may not be "used" to the former client's disadvantage unless the information is "generally known." *Id.* r. 1.9(c)(1). This "generally known" exception to the duty of former-client confidentiality is limited. It applies only (1) to the use, rather than the disclosure or revelation, of former-client information and (2) if the information has become (a) widely recognized by members of the public in the relevant geographic area or (b) widely recognized in the former client's industry, profession, or trade. Information is not "generally known" simply because it has been discussed in open court or is available in court records, libraries, or other public repositories of information. *See* ABA Standing Comm. on Ethics & Prof'l Resp., Formal Op. 479 (Dec. 15, 2017). *But see infra* notes 32–34 and accompanying text (discussing different usage in the Restatement (Third) of the Law Governing Lawyers).

lawyer–client communications, lawyer work product, and much more (even some publicly available information, as explained below).[29] Indeed, the breadth of the phrase's application may be surprising to many, particularly when compared to the narrow scope of the attorney–client privilege and the work-product doctrine.

The law of evidence has created the attorney–client privilege, which—unless waived—protects confidential communications between a lawyer and a client for the purpose of seeking legal advice. Further, the judge-made work-product doctrine generally protects a lawyer's mental impressions in litigation or in anticipation of litigation from disclosure. Thus, the attorney–client privilege and work-product doctrine operate as shields that allow both lawyer and client to refuse to disclose these particular categories of confidential information, even despite a subpoena.[30]

The Official Comment to Model Rule 1.6 explicates the breadth of "information relating to the representation of a client":

> [3] The principle of client–lawyer confidentiality is given effect by related bodies of law: the attorney–client privilege, the work product doctrine and the rule of confidentiality established in professional ethics. The attorney–client privilege and work product doctrine apply in judicial and other proceedings in which a lawyer may be called as a witness or otherwise required to produce evidence concerning a client. *The rule of client–lawyer confidentiality applies in situations other than those where evidence is sought from the lawyer through compulsion of law*. The confidentiality rule, for example, applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source. A lawyer may not disclose such information except as authorized or required by the Rules of Professional Conduct or other law. . . .
>
> [4] Paragraph (a) prohibits a lawyer from revealing information relating to the representation of a client. *This prohibition also applies to disclosures by a lawyer that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person. . . .*[31]

29. Model Rule r. 1.6.

30. See the excellent discussion of this distinction in Stephen Gillers, Regulation of Lawyers: Problems of Law and Ethics 32–33 (11th ed. 2018). "Rule 1.6(a) defines a category of information (described as 'information relating to the representation of a client') that a lawyer may not *voluntarily* reveal unless there is an exception (as in, e.g., Rule 1.6[b], 1.13[c], and 3.3[c] . . .) or the client has given consent, which may be implied." *Id.* "But if a question calls for information protected by the attorney-client (or other) privilege, both a lawyer and a client can 'refuse to disclose' it." *Id.*

31. Model Rules r. 1.6 cmts. [3–4] (emphasis added). Part of paragraph [14] of the Scope section is generally relevant:

> [14] The Rules of Professional Conduct are rules of reason. They should be interpreted with reference to the purposes of legal representation and of the law itself. Some of the rules are imperatives, cast in the terms "shall" or "shall not." These define proper conduct for purposes of professional discipline. Others, generally cast in the term "may," are permissive and define areas under the Rules in which the lawyer has discretion to exercise professional judgment. No disciplinary action should be taken when the lawyer chooses not to act or acts within the bounds of such discretion.

Id. scope cmt. [14].

The Restatement (Third) of the Law Governing Lawyers[32] ("Restatement") has slightly different language describing the scope of confidential client information:

> § 59. Definition of "Confidential Client Information"
>
> Confidential client information consists of information relating to representation of a client, *other than information that is generally known*.
>
> Comment:
>
> (b) *Kinds of confidential client information*. . . . This definition covers all information relating to representation of a client, whether in oral, documentary, electronic, photographic, or other forms. It covers information gathered from any source, including sources such as third persons whose communications are not protected by the attorney–client privilege (see § 70). It includes work product that the lawyer develops in representing the client, such as the lawyer's notes to a personal file, whether or not the information is immune from discovery as lawyer work product. . . . *The definition includes information that becomes known by others, so long as the information does not become generally known*.
>
> * * *
>
> *d. Generally known information*. Confidential client information does not include information that is generally known. . . . Information might be generally known at the time it is conveyed to the lawyer or might become generally known thereafter. At the same time, the fact that information has become known to some others does not deprive it of protection if it has not become generally known in the relevant sector of the public.
>
> Whether information is generally known depends on all circumstances relevant in obtaining the information. Information contained in books or records in public libraries, public-record depositaries such as government offices, or in publicly accessible electronic-data storage is generally known if the particular information is obtainable through publicly available indexes and similar methods of access.[33]

The Restatement has a version of the lawyer's duty to safeguard confidential information that is different from Model Rule 1.6(c):

> § 60. A Lawyer's Duty to Safeguard Confidential Client Information
>
> * * *
>
> (b) the lawyer must take steps reasonable in the circumstances to protect confidential client information against impermissible use or disclosure by the lawyer's associates or agents that may adversely affect a material interest of the client or otherwise than as instructed by the client.[34]

32. RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 59 (AM. LAW. INST. 2000) (emphasis added).

33. For a discussion of the term "generally known" in the context of the scope of Model Rule 1.6 (c), as it relates to former clients, see *supra* note 27.

34. RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 60.

It is important to understand that although there are differing nuances between the Model Rules and the principles set forth in the Restatement, the latter is advisory only. It has no "teeth." Of course, neither do the ABA's Model Rules, which would have "teeth" only if adopted in the lawyer's jurisdiction. Still, the Restatement and the Model Rules give good guidance and provide useful context.

The Ethical Responsibilities of Law Firms, Including Corporate Law Departments

The foregoing discussion relates to the ethical obligations of the individual lawyer. It is extremely important, however, to put these individual-lawyer responsibilities in the supervisory context of the responsibility of the managing hierarchy of a corporate law department or external law firm. In terms of who "takes the fall" for a data breach in a large law firm or corporate law department, one should look to those at the top. Model Rules 5.1 (Responsibilities of Partners, Managers, and Supervisory Lawyers) and 5.3 (Responsibilities Regarding Nonlawyer Assistance) address these hierarchical responsibilities as follows:

> Model Rule 5.1. Responsibilities of partners, managers, and supervisory lawyers.
>
> (a) A partner in a law firm,[35] and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, *shall* make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.
>
> (b) A lawyer having direct supervisory authority over another lawyer *shall* make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.[36]

As to the responsibilities of the lawyers at the top of the hierarchical pyramid of the corporate law department (i.e., the general counsel) and in a law firm (i.e., the management committee or equivalent), the overarching concept is that a high ethical "tone at the top" is a key cultural expectation. In law firms, the tone at the top is a way of reinforcing the professionalism that is part of the "business" of the firm. For corporations and like organizations, the general counsel and her team are there to reinforce the core values of the firm as well as provide competent legal advice.

The corporate general counsel and her corporate law department management team are often regarded as the "guardians of the corporate integrity."[37] The

35. Note that the terms "firm" and "law firm" are defined in the Model Rules Terminology section to include corporate law departments:

> (c) "Firm" or "law firm" denotes a lawyer or lawyers in a law partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization or the legal department of a corporation or other organization.

36. Model Rules r. 5.1 (emphasis added).

37. E. Norman Veasey & Christine T. DiGuglielmo, Indispensable Counsel: The Chief Legal Officer in the New Reality 97–98 (2012); *see also* Ben W. Heineman, Jr., The Inside Counsel Revolution 55–89 (2016).

general counsel must be a key point person for monitoring and promoting ethical conduct throughout the corporate organization. In fact, several prominent general counsel have endorsed this principle:

> The general counsel's job is to be a champion of integrity, compliance, and the rule of law. That is the way the organization looks upon the general counsel. That is a tremendously important role.[38]

Model Rule 5.1 and Model Rule 5.3, discussed below, apply equally to corporate law departments and to outside counsel.[39] For example, in view of the progress of learning and the application of ethics responsibilities today, one would be hard-pressed to excuse law-firm management in the M&A space from not having top-of-the-line cyber-protection to prevent any compromise of communications or data, including the interception of sensitive merger-negotiation telephone discussions between sophisticated law firms.[40] An excellent 2017 book entitled *Guide to Cybersecurity Due Diligence in M&A Transactions* gives many examples of necessary precautions against cyberattack. One such example of managerial responsibility is as follows:

> 2.1. Senior Management and Board Involvement
>
> Is senior management actively involved in overseeing the development, implementation, and maintenance of the target's cybersecurity program, and what is the role of the board in overseeing the target's cybersecurity program?
>
> The strength of a cybersecurity program depends in large part on the "buy-in" and role of senior management in overseeing the program. A best-practices cybersecurity program is one in which c-suite executives and the board of directors are regularly apprised of the cybersecurity risks the company faces; understand the techniques that the IT specialists at the company have adopted to address those risks; and signal to the rest of the organization that cybersecurity is a corporate priority. A lack of involvement by these decision makers might signal that the company does not take cybersecurity seriously, and that critical decisions are not made at senior levels of the organization.[41]

38. Veasey & Di Guglielmo, *supra* note 37, at 97 (quoting Bracket Denniston, former General Counsel of General Electric Co.).

39. *See, e.g.*, Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information (Ass'n Corp. Couns. Mar. 2017); Brad Brian & Grant Davis-Denny, *Data Breaches and the Role of the In-House Attorney*, U.S. News—Best Law: Best L. Firms 2016, Oct. 22, 2015, at 36; The General Counsel's Guide to Digital Defense (Guerrero Howe Custom Media, Sept. 20, 2016); Kevin LaCrois, *Guest Post: Three Cybersecurity Lessons From Yahoo's Legal Department Woes*, D&O Diary (Mar. 30, 2017), https://www.dandodiary.com/2017/03/articles/cyber-liability/guest-post-three-cybersecurity-lessons-yahoos-legal-department-woes; Richard May, What Law Firms Need to Know About Cyber Crime and Coverage (2017); U.S. Dep't of Justice Cybersecurity Unit, Best Practices for Victim Response and Reporting of Cyber Incidents (Apr. 2015), https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal _division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf.

40. *See supra* notes 10–12 and accompanying text (providing a related "horror story").

41. Thomas J. Smedinghoff & Roland L. Trope, Guide to Cybersecurity Due Diligence in M&A Transactions 91 (2017).

In addition to emphasizing the ethical supervision of lawyers under Model Rule 5.1, the Ethics 20/20 Commission Report zeroes in on the management and supervision of nonlawyer assistance for law firms and corporate law departments.[42] This is an increasingly important area because firms make extensive use not only of in-house paralegals but also outside assistance. As a result, Model Rule 5.3 has become progressively more relevant. It provides:

> Model Rule 5.3. Responsibilities Regarding Nonlawyer Assistance.[43]
>
> With respect to a nonlawyer employed or retained by or associated with a lawyer:
>
> (a) a partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;
>
> (b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and
>
> (c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:
>
> (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
>
> (2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.[44]

The high-velocity and technologically driven law practice of today increasingly involves nonlawyers. Beyond the expanding but traditional use of paralegals and other nonlawyers in firms, there is a trend of individual lawyers, law firms, and corporate law departments turning to nonlawyers for assistance. That assistance is often in the outsourced areas of litigation support and technical services.[45] Official Comments [3] and [4] to Model Rule 5.3 emphasize the steps lawyers must take when outsourcing tasks:

> Official Comment
>
> [3] *Nonlawyers Outside the Firm*. A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the

42. *See supra* note 15.

43. Interestingly, the heading for Model Rule 5.3 was changed as a result of the Ethics 20/20 Commission Report. The old term "Nonlawyer Assistants" was changed to "Nonlawyer Assistance" to reflect the expanded concept that assistance often comes from outside the firm.

44. Model Rules r. 5.3.

45. *See, e.g.*, Michael J. Progar, *A Lawyer's Obligations When Outsourcing Services*, 18 I.D.C.Q. 22, 22–25 (2008); Mark Dreher, *Multi-State Survey of Ethical Opinions Regarding Legal Process Outsourcing*, Butler Snow (Apr. 1, 2009), https://3epjwm3sm3iv250i67219jho-wpengine.netdna-ssl.com/wp-content/uploads/pdfs/attorney_publications/case-law-multi-state-survey-of-ethical-opinions-regarding-legal-process-outsourcing.pdf.

> retention of an investigative or paraprofessional service, hiring a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an internet-based service to store client information. *When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations*. The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality. See also Rules 1.1 (competence), 1.2 (allocation of authority), 1.4 (communication with client), 1.6 (confidentiality), 5.4(a) (professional independence of the lawyer), and 5.5(a) (unauthorized practice of law). *When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer*.
>
> [4] Where the client directs the selection of a particular nonlawyer service provider outside the firm, the lawyer ordinarily should agree with the client concerning the allocation of responsibility for monitoring as between the client and the lawyer. See Rule 1.2. When making such an allocation in a matter pending before a tribunal, lawyers and parties may have additional obligations that are a matter of law beyond the scope of these Rules.[46]

In sum, individual lawyers and law-firm managers have ethical duties to maintain competency and confidentiality in an increasingly technical world and ensure that nonlawyers working with them are aware of, and comply with, those duties as well.

Getting Expert Assistance

As noted, this article is not intended to teach technical subject matter. It is intended only as a reminder that competent lawyers should keep abreast of the benefits and risks of technology and must make reasonable efforts to protect client information. In so doing, a lawyer should regularly seek and heed expert advice and assistance.[47]

> Getting expert help is a recurring theme (as well as good advice) in ethics opinions on this subject. Arizona Bar Opinion 09-04 (Dec. 2009) reminds lawyers that, if they provide an online file storage and retrieval system for client access of documents, then they must take reasonable precautions to protect the security and confidentiality of client documents and information. With respect to a lawyer's obligation to be competent, the opinion noted that "[i]t is also important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field."

46. Model Rule r. 5.3 cmts. [3–4] (emphasis added).

47. Peter Geraghty & Lucian T. Pera, *Lawyers' Obligations to Provide Data Security Arising from Ethics Rules and Other Law, in* The ABA Cybersecurity Handbook, *supra* note 4, at 115, 124–25.

> Moreover, competence requires continued vigilance and learning, as technology advances, in order to comply with a lawyer's duties under the ethics rules. Again, the Arizona Bar also reminded lawyers that "[a]s technology advances occur, lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients' documents and information." In other words, lawyers may not assume that their ignorance about technology will be a recognized excuse for their failure to learn, and stay up-to-date, about technology related to a client's electronically stored information."[48]

The individual lawyer and the law firm both need to have competent and technically trained in-house staff or outside contractors working with them on a regular basis.[49]

Valuable Explications Found in Formal Opinions

The entire regime of the professional-responsibility apparatus can be efficiently analyzed through the lens of the formal opinions of the Bars of the various states and the ABA Standing Committee on Ethics and Professional Responsibility ("SCEPR"). The leading example is the 2017 SCEPR Formal Opinion 477R.[50] This ABA opinion is an important explication of Model Rule 1.6(c) and Official Comment [8] to Model Rule 1.1, providing excellent advice for lawyers and law firms.[51] Opinion 477R states in part:

> Each device and each storage location offer an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation, and thus implicate a lawyer's ethical duties.
>
> At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology," and the confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," lawyers must exercise reasonable efforts when using technology in communication about client matters.[52]

The opinion goes on to specify what lawyers should do:

1. Understand the nature of the threat. ["Reasonable efforts" in high-risk scenarios generally means that greater effort is warranted.]
2. Understand how client confidential information is transmitted and where it is stored.

48. *Id.*

49. It is not appropriate for me to mention the identity of potential technical experts that a firm might consider retaining. But the appendices to *The Cybersecurity Handbook* contain technical guidance to issues that an expert might address—especially Appendices Q and R. *See* The ABA Cybersecurity Handbook, *supra* note 4 (providing the appendices); *see also id.* at 437–46 (providing Appendices Q and R).

50. ABA Comm. on Ethics & Prof'l Resp., Formal Op. 477R (May 22, 2017) [hereinafter Opinion 477R].

51. *See* Geraghty & Pera, *supra* note 47, at 115–18.

52. *Id.*

3. Understand and use reasonable electronic security measures.
4. Determine how electronic communications about client matters should be protected. [In some circumstances, a client's lack of technological sophistication or the limitations of technology available to the client may require a warning to the client or alternative nonelectronic forms of communication altogether such as a telephone call or face-to-face communication.]
5. Label client confidential information. [Model Rule 4.4 obligates a lawyer who "knows or reasonably should know" that he or she has received an inadvertently sent "document or electronically stored information relating to the representation of the lawyer's client" to promptly notify the sending lawyer.[53]]
6. Train lawyers and nonlawyer assistants in technology and information security.
7. Conduct due diligence on vendors providing communication technology.[54]

In the *Cybersecurity Handbook*, Paul Rosenzweig provides additional suggestions. Each law firm needs to analyze its portals of potential vulnerability, create a plan to patch or fix those areas, upgrade the entire electronic security system, continually monitor areas of potential weakness or vulnerability, and take at least some of the following actions:

1. Identify information assets;
2. Conduct periodic risk assessments;
3. Develop and implement appropriate security plans;
4. Provide training and education;
5. Monitor and test security controls;
6. With outside experts, review and adjust security program; and
7. Oversee third-party service-provider arrangements.[55]

In 2018, SCEPR issued a further opinion (Formal Op. 483) regarding a lawyer's *post-breach* responsibilities—an opinion that all lawyers should heed.[56] Here are a few excerpts from that opinion:

> In Formal Opinion 477R, this Committee explained a lawyer's ethical responsibility to use reasonable efforts when communicating [confidential client] information using the Internet. This opinion picks up where Opinion 477R left off, and discusses an attorney's ethical obligations when a data breach exposes [confidential client] information. This opinion focuses on an attorney's ethical obligations after a data breach, and it addresses only data breaches that involve information relating to the representation of a client. . . .

53. Model Rule 4.4. There may be further steps taken in federal litigation by the recipient of inadvertently sent information. *See* Fed. R. Evid. 502; Fed. R. Civ. P. 26(b)(5)(B).
54. Opinion 477R, *supra* note 50, at 5–9.
55. Paul Rosenzweig, *Understanding Technology: What Every Lawyer Needs to Know About the Cyber Network*, *in* The ABA Cybersecurity Handbook, *supra* note 4, at 76, 76–87.
56. ABA Comm. on Ethics & Prof'l Resp., Formal Op. 483 (Oct. 17, 2018).

> However, compliance with statutes such as state breach notification laws, HIPAA, or the Gramm-Leach-Bliley Act does not necessarily achieve compliance with ethics obligations. Nor does compliance with lawyer regulatory rules *per se* represent compliance with breach response laws. As a matter of best practices, lawyers who have suffered a data breach should analyze compliance separately under every applicable law or rule.
>
> * * *
>
> A data breach for the purposes of this opinion means a data event where material [confidential client] information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode. . . .
>
> * * *
>
> *The strong client protections mandated by Model Rule[s] 1.1, 1.6, 5.1 and 5.3, particularly as they were amended in 2012 to account for risks associated with the use of technology, would be compromised if a lawyer who experiences a data breach that impacts [confidential client] information is permitted to hide those events from their clients. . . .*
>
> * * *
>
> Even lawyers who, (i) under Model Rule 1.6(c), make "reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," (ii) under Model [R]ule 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data breach under Model Rule 1.4 in sufficient detail to keep clients "reasonably informed" and with an explanation "to the extent necessary to permit the client to make informed decisions regarding the representations."[57]

If Model Rules 1.6(c), 5.1, and 5.3 and the Official Comment to Model Rule 1.1 have been adopted by the highest authority in the lawyer's jurisdiction, those embarrassing consequences could include exposure to sanctions for ethical violations, possible violations of state and federal statutes, and possible exposure to class actions or other litigation.

Effect of the Model Rules When Adopted in the Lawyer's Jurisdiction

Clearly, a lawyer's failure to "make reasonable efforts" to prevent disclosure or unauthorized access to client information under Model Rule 1.6(c) has an official professional-conduct impact on a lawyer if an equivalent rule has been adopted by the highest authority in the lawyer's jurisdiction. The Model Rules might be relegated to aspirational status and would have no "teeth" as a disciplinary matter, unless adopted by the highest authority in the lawyer's jurisdiction. If

57. *Id.* (emphasis added).

adopted by that authority, the state disciplinary rules could be the basis for sanctions.[58]

Nevertheless, there can be civil actions in the nature of a class or individual actions where a lawyer is sought to be held accountable in court:

> There can be no doubt that traditional bodies of law used to hold lawyers and law firms accountable for certain harms resulting from their conduct can be used for data and other cybersecurity breaches. With respect to harms suffered by clients, the law offers an obvious path for malpractice liability to a client predicated on a breach of confidentiality and for liability to a client for breach of the fiduciary duty of confidentiality. Inadvertent disclosures of confidential information have, under such principles, led to claims against lawyers and law firms. Of course, intentional misappropriation and misuse of client confidential information can lead not only to claims on these theories, but also to claims under other theories premised upon intentional misconduct, both common law and statutory. Under all these theories, however, it is sometimes quite difficult for claimants to prove causation to the extent required by law.[59]

It has been cogently recognized that the legal standard for "reasonable security" is an emerging concept, which is widely understood to be process related. It thus requires a case-by-case, fact-based assessment of specific risks and appropriate security measures responsive to those risks.[60]

Regardless of whether a lawyer is practicing in a jurisdiction that has adopted the new Model Rules or Official Comments, they must be circumspect and careful when it comes to protecting client information.[61] In my opinion, the examples are legion: negligence with a briefcase or laptop, carelessness with a smart phone or other device during international travel, etc.[62] Also, problems can arise

58. Due to the confidentiality of the processes of disciplinary counsel in the various jurisdictions, it is impracticable to cite professional-conduct cases pending before disciplinary counsel. Only where a disciplinary proceeding has reached the highest court of the jurisdiction does it become public, and I do not know of any public opinions in this area.

59. Geraghty & Pera, *supra* note 47, at 115, 126–27.

60. Thomas J. Smedinghoff & Ruth Hill Bro, *Lawyers' Legal Obligations to Provide Data Security*, *in* The ABA Cybersecurity Handbook, *supra* note 4, at 61, 73–81; *see also* Kevin P. Kalinich & James L. Rhyner, *Cyber Insurance for Law Firms and Legal Organizations*, *in* The ABA Cybersecurity Handbook, *supra* note 4, at 313, 314 (citing Shore v. Johnson & Bell, Ltd., No. 1:16-cv-04363 (N.D. Ill. Apr. 15, 2016) (unsealed Dec. 9, 2016)).

61. The lawyer's or law firm's ethical failure to take reasonable steps to protect client information may be evidence of a waiver of the attorney–client privilege or the basis of a legal-malpractice or other civil-liability claims. But those analyses may involve complicated questions that should be examined separately.

> [19] Failure to comply with an obligation or prohibition imposed by a Rule is a basis for invoking the disciplinary process.
>
> [20] Violation of a Rule should not itself give rise to a cause of action against a lawyer nor should it create any presumption in such a case that a legal duty has been breached. . . . Nevertheless, since the Rules do establish standards of conduct by [for] lawyers, a lawyer's violation of a Rule may be evidence of breach of the applicable standard of conduct.

Model Rules *scope* [19–20].

62. In particular, international travel can be problematic for the lawyer who brings her smart phone, laptop, or other device containing confidential client information across international borders—not

for lawyers who carelessly rely on old software, use "soft" passwords, carelessly open email attachments or links, misplace or lose their mobile devices, or carelessly use social media, such as a blog.[63]

Adoption among the jurisdictions of Model Rule 1.6(c) and Official Comment to Model Rule 1.1 is uneven, to put it mildly.[64] In researching the patchwork landscape across the jurisdictions when it comes to the adoption of Model Rule 1.6(c) or its equivalent, one will probably find that thirty-five (roughly 70 percent) of the fifty-one jurisdictions (the fifty states and the District of Columbia) have formally adopted Model Rule 1.6(c) in its exact or substantially equivalent form.[65] There appear to be sixteen (roughly 30 percent) of the jurisdictions that have *not* adopted Model Rule 1.6(c) or its equivalent.[66]

Similarly, thirty-six jurisdictions[67] (also roughly 70 percent) have embraced, in one form or another, the expectation expressed in Official Model Rule 1.1 Comment [8] that lawyer competence means, among other competencies, that lawyers are expected to keep abreast of the benefits and risks associated with relevant technology.[68] Fifteen jurisdictions (also roughly 30 percent) have not adopted such a tech-competence statement (like Comment [8] to Model Rule 1.1) in

only to Russia or China but also to Canada, where border agents may be empowered to access data brought across the border from the United States. *See* Daniel Crothers & Barbara Gillers, *Electronic Device Advisory for Mid-Year Attendees*, AM. B. ASS'N (Jan. 10, 2018), https://www.americanbar.org/content/dam/aba/events/meetings_travel/scerp-electronic-device-advisory-djcbsg-1-10-18.authcheckdam.pdf; *ABA Urges Homeland Security Department to Modify Procedures for Searching Lawyers' Electronic Devices at U.S. Border Crossings*, AM. B. ASS'N WASH. LETTER (May 31, 2017); *As Border Searches of Electronics Rise, Here's How to Protect Your Clients' Data*, YOUR ABA (Sept. 5, 2017); Am. Bar Ass'n Media Relations, *Take Precautions to Protect Your Clients When Bringing Devices Across Borders, Experts Say,* INT'L L. NEWS (Aug. 24, 2017); *CBP Addresses ABA Concerns in Revised Standards for Borders [sic] Searches of Lawyer's Electronic Devices*, AM. B. ASS'N WASH. LETTER (Feb. 28, 2018); Sharon D. Nelson & John W. Simek, *Hot Buttons—Disasters and Data Breaches: The ABA Speaks*, L. PRAC. MAG. (Nov. 1, 2018).

63. *See, e.g.*, ABA Comm. on Ethics & Prof'l Resp., Formal Op. 480 (Mar. 6, 2018).

64. *See Variations of the ABA Model Rules of Professional Conduct, Rule 1.6: Confidentiality of Information*, AM. B. ASS'N (Sept. 2019), https://www.americanbar.org/groups/professional_responsibility/policy/rule_charts.

65. They are: Alaska, Arkansas, Arizona, Colorado, Connecticut, Delaware, Florida, Idaho, Illinois, Iowa, Kansas, Louisiana, Massachusetts, Minnesota, Missouri, Montana, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Tennessee, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.

66. They are: Alabama, California, the District of Columbia, Georgia, Hawaii, Indiana, Kentucky, Maine, Maryland, Michigan, Mississippi, Nebraska, Rhode Island, South Carolina, Texas, and Vermont.

67. They are: Alaska, Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Massachusetts, Minnesota, Missouri, Montana, Nebraska, New Hampshire, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.

68. *See* Robert Ambrogi, *Tech Competence*, LAWSITES, https://www.lawsitesblog.com/tech-competence (last visited Oct. 4, 2019). In addition, California, through Formal Opinion No. 2015-193 of its *own* state bar, more narrowly requires lawyers who represent clients in litigation either to be competent in e-discovery or be associated with a lawyer who is competent in the relevant area. *Id.*

their Rules of Professional Conduct.[69] Five of the fifteen jurisdictions have not adopted *any* formal comments to their rules.[70]

If a lawyer's licensing jurisdiction has adopted a rule such as Model Rule 1.6(c) or its equivalent, the Rule has "teeth." The lawyer is governed by that rule and is *required* to follow it, because the rule states that the lawyer ("shall") make such reasonable efforts.[71] A lawyer's failure to follow that rule could result in a disciplinary violation under that jurisdiction's version of Model Rule 8.4(a), which makes it professional misconduct for a lawyer to violate a rule of professional conduct.[72]

It would be interesting to know the pertinent anecdotal background facts of some of the jurisdictions that did not adopt Model Rule 1.6(c). As was observered at the Ethics 2000 debates, certain exceptions to Model Rule 1.6 were controversial.[73] That general controversy seemed to be fueled, in part, by disparate scholarly philosophies on the need for or the wisdom of certain exceptions to Model Rule 1.6(b) and overarching concerns about keeping confidences inviolate and being wary of adopting all but the most necessary exceptions (such as Model Rule 1.6(b)(1) regarding death or substantial bodily harm). By contrast, however, it is difficult to see why there would be reluctance to embrace a requirement mandating that measures be taken to protect confidential client

69. They are: Alabama, California (*see supra* note 62), the District of Columbia, Georgia, Hawaii, Maine, Maryland, Michigan, Mississippi, New Jersey, Nevada, Oregon, Rhode Island, South Carolina, and South Dakota. Email from Mary McDermott, Esq., of the Policy Implementation Comm., Am. Bar Ass'n Ctr. for Prof'l Responsibility, to E. Norman Veasey (Aug. 6, 2019) (on file with author).

70. They are: New Jersey, Nevada, Oregon, South Dakota, and Louisiana. *But see* Louisiana State Bar Pub. Op. 19-RPCC-021. Email from Mary McDermott, Esq., of the Policy Implementation Comm., Am. Bar Ass'n Ctr. for Prof'l Responsibility, to E. Norma Veasey (Aug. 6, 2019) (on file with author).

71. There may be a choice-of-law issue if a lawyer admitted in State A, which has not adopted Model Rule 1.6(c), is also performing professional services in State B, which has adopted the rule. *See generally* MODEL RULES r. 8.5. The rule states:

> Rule 8.5: Disciplinary Authority; Choice of Law
>
> (a) Disciplinary Authority. A lawyer admitted to practice in this jurisdiction is subject to the disciplinary authority of this jurisdiction, regardless of where the lawyer's conduct occurs. A lawyer not admitted in this jurisdiction is also subject to the disciplinary authority of this jurisdiction if the lawyer provides or offers to provide any legal services in this jurisdiction. A lawyer may be subject to the disciplinary authority of both this jurisdiction and another jurisdiction for the same conduct.

72. Model Rule 8.4(a) states: "It is professional misconduct for a lawyer to:

> (a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another . . . ."

MODEL RULES r. 8.4(a).

73. This was particularly true of Model Rule 1.6(b)(2), which permits a lawyer to disclose client information under certain circumstances

> (2) [t]o prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services . . . .

MODEL RULES r. 1.6(b)(2)

information from unauthorized access.[74] Any theories about the reasons for the reluctance to adopt Model Rule 1.6(c) in the majority of jurisdictions that have not adopted it would be sheer speculation at this point.

What if a lawyer's jurisdiction has *not* adopted Model Rule 1.6(c), and the lawyer fails to make a reasonable effort to prevent unauthorized use of client information, resulting in a cyberattack that compromises a client's confidential information? One could argue that Model Rule 1.6(c) and state-based rules patterned after it are codifications of pre-existing principles of professional conduct gleaned from the context of the rules and professional responsibility generally,[75] thus establishing a professional *expectation* that lawyers will make reasonable efforts to protect client information.

But can there be an official professional-misconduct sanction or other consequences under a state-based equivalent of Model Rule 8.4(a) if a specific black-letter rule that the lawyer "*shall* make reasonable efforts" to protect client information against cyberattack has not been formally adopted in a given jurisdiction? More important, is testing the enforceability of a concept not attached to a black-letter rule—especially where client information has been compromised—a good idea? The *best-practices* approach is for lawyers and firm managers to operate as if Model Rule 1.6(c) and Comment [8] to Model Rule 1.1 were adopted by the highest authority in their jurisdiction, whether or not they actually were. Enforcement is perhaps another issue for another day.

Conclusion

The cybercrime threat, which is menacing and damaging law firms and businesses, is a clear and present danger. There are many resources available for study, not only as to the awareness of the peril but also as to the steps that must be taken for prevention and mitigation.[76] This article is intended to be

74. In analyzing the "scorecard" relating to states' adoption of Model Rule 1.6(c), as inspired by the Ethics 20/20 Report, there are a number of jurisdictions that also chose not to adopt Model Rule 1.6(b)(7). One can only speculate about the diverse views in those jurisdictions, aside from the fact that the process of considering new ethics rules can be contentious. Model Rule 1.6(b)(7) permits a lawyer to reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary, such as:

> (7) to detect and resolve conflicts of interest arising from the lawyer's change of employment or from changes in the composition or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

Model Rules r. 1.6(b)(7).

75. *See, e.g.,* Model Rules r. 1.1 (relating to competence), 1.15 (relating to safeguarding property), 1.3 (relating to diligence), 1.4 (relating to communication), 1.6 (relating to confidential client information generally), and 5.1 and 5.3 (providing supervisory rules); *see also id. scope* [16] ("The Rules do not, however, exhaust the moral and ethical considerations that should inform a lawyer, for no worthwhile human activity can be completely defined by legal rules. The Rules provide [a] framework for the ethical practice of law."); *In re* Holley, 729 N.Y.S.2d 128 (Sup. Ct. 2001).

76. *See, e.g.*, Jeffrey Allen & Ashley Hallene, *Protecting Your Email and Confidential Information*, Am. B. Ass'n J. (Jan. 1, 2019); Sean C. Griffin, *Attorneys' Liability for Data Breaches*, For the Defense, Nov. 2016, at 14; David Hudson, Jr., *Lawyers Must Secure Client Communications from Cyber Breaches*, Am. B. Ass'n J. (July 1, 2017); Alan Charles Raul, *Cybersecurity—It's Not Just About "National Security"*

one of the many wake-up calls for lawyer awareness and action. In my opinion, business lawyers, firm managers, and particularly their clients should make a culture of strong cybersecurity a top priority.[77]

Also, in my opinion, the jurisdictions that have not adopted Model Rule 1.6(c) and the Official Comment to Model Rule 1.1 should consider doing so without substantial delay, so the adoption of these Rules and Comments can be universal.

Anymore: "Directors Desk" and Other Incidents Sound Wake-Up Call for the Executive Suite and Board Room, 10 PRIVACY & SEC. L. REP. (BNA) 347 (Feb. 28, 2011); SEC. FOR BUS. INNOVATION COUNCIL, TRANSFORMING INFORMATION SECURITY: DESIGNING A STATE-OF-THE-ART EXTENDED TEAM (Sept. 2016); Daniel J. Siegel, *Law Firms Must Be Proactive to Prevent Cyberattacks*, LEGAL INTELLIGENCER (Apr. 26, 2018); Drew Simshaw & Stephen Wu, Ethics and Cybersecurity: Obligations to Protect Client Data, Presented at the National Symposium on Technology in Labor and Employment Law, San Francisco, CA (Mar. 15–17, 2015); Jason Tashea, *Lawyers Have an Ethical Duty to Safeguard Confidential Information in the Cloud*, AM. B. ASS'N J. (Apr. 1, 2018).

77. THE GENERAL COUNSEL'S GUIDE TO DIGITAL DEFENSE, *supra* note 39; RICHARD MAY, INTEGRO WHITE PAPER: WHAT LAW FIRMS NEED TO KNOW ABOUT CYBER CRIME AND COVERAGE (2017), https://integrogroup.com/uploads/white_papers/Integro_Law_Cyber_Crime_White_Paper_1453_August_2017.pdf.