



DATE DOWNLOADED: Wed Feb 28 13:26:38 2024

SOURCE: Content Downloaded from [HeinOnline](#)

Citations:

Please note: citations are provided as a general guideline. Users should consult their preferred citation format's style manual for proper citation formatting.

Bluebook 21st ed.

Ethan S. Burger, Professional Responsibility, Legal Malpractice, Cybersecurity, and Cyber-Insurance in the COVID-19 Era, 11 ST. MARY'S J. ON LEGAL MALPRACTICE & ETHICS 234 (2021).

ALWD 7th ed.

Ethan S. Burger, Professional Responsibility, Legal Malpractice, Cybersecurity, and Cyber-Insurance in the COVID-19 Era, 11 span style='font-size:13px;'>St. Mary's J. on Legal Malpractice & Ethics 234 (2021).

APA 7th ed.

Burger, E. S. (2021). Professional responsibility, legal malpractice, cybersecurity, and cyber-insurance in the covid-19 era. St. Mary's Journal on Legal Malpractice and Ethics, 11(2), 234-310.

Chicago 17th ed.

Ethan S. Burger, "Professional Responsibility, Legal Malpractice, Cybersecurity, and Cyber-Insurance in the COVID-19 Era," St. Mary's Journal on Legal Malpractice and Ethics 11, no. 2 (2021): 234-310

McGill Guide 9th ed.

Ethan S. Burger, "Professional Responsibility, Legal Malpractice, Cybersecurity, and Cyber-Insurance in the COVID-19 Era" (2021) 11:2 span style='font-size:13px;'>St Mary's J on Legal Malpractice & Ethics 234.

AGLC 4th ed.

Ethan S. Burger, 'Professional Responsibility, Legal Malpractice, Cybersecurity, and Cyber-Insurance in the COVID-19 Era' (2021) 11(2) St. Mary's Journal on Legal Malpractice and Ethics 234

MLA 9th ed.

Burger, Ethan S. "Professional Responsibility, Legal Malpractice, Cybersecurity, and Cyber-Insurance in the COVID-19 Era." St. Mary's Journal on Legal Malpractice and Ethics, vol. 11, no. 2, 2021, pp. 234-310. HeinOnline.

OSCOLA 4th ed.

Ethan S. Burger, 'Professional Responsibility, Legal Malpractice, Cybersecurity, and Cyber-Insurance in the COVID-19 Era' (2021) 11 span style='font-size:13px;'>St Mary's J on Legal Malpractice & Ethics 234 Please note: citations are provided as a general guideline. Users should consult their preferred citation format's style manual for proper citation formatting.

-- Your use of this HeinOnline PDF indicates your acceptance of HeinOnline's Terms and Conditions of the license agreement available at

<https://heinonline.org/HOL/License>

# ARTICLE

*Ethan S. Burger*

## Professional Responsibility, Legal Malpractice, Cybersecurity, and Cyber-Insurance in the COVID-19 Era

**Abstract.** In response to the COVID-19 outbreak, law firms conformed their activities to the Centers for Disease Control and Prevention (CDC), Occupational Safety and Health Administration (OSHA), and state health authority guidelines by immediately reducing the size of gatherings, encouraging social distancing, and mandating the use of protective gear. These changes necessitated the expansion of law firm remote operations, made possible by the increased adoption of technological tools to coordinate workflow and administrative tasks, communicate with clients, and engage with judicial and governmental bodies.

Law firms' increased use of these technological tools for carrying out legal and administrative activities has implications for their staffing needs, office space requirements, and management/supervisory procedures. Actions taken in each of these areas give rise to certain risks, which are by-products of the COVID-19 virus, albeit, not caused by it. Due to the pandemic, law firms have had to address certain secondary (i.e., not health-related) risks arising from (i) non-compliance with professional conduct norms, (ii) legal malpractice, (iii) increased cybersecurity vulnerability, and (iv) need for cyber-insurance. In the twelve months after March 2020, there was an overall drop in lawyer productivity. It is not clear how long clients will accept this situation to continue.

What has been the impact of COVID-19 on law firms? It seems there has been a growing gap between the "haves" and the "have-nots," with the former getting a bulk of the "high-end" work. In the near term, remote operations

combined with personnel reductions seem to have had a negative impact on most law firms' efficiency and, ultimately, revenue. It should not be a surprise that certain law firms have found that adopting "austerity measures" can ensure profitability.

Remote operations make law firms more vulnerable to cyber-attacks. Most law firms tend to disregard these risks unless their clients or regulators insist on their adoption of new cybersecurity measures. While a dramatic increase in successful cyber-attacks on law firms and other private-sector organizations might change this situation, profitability will remain the top objective of law firm partners.

As a result, it is unlikely that law firms will increase their investment in cybersecurity in the form of expensive equipment, software, services from outside contractors, and cyber-insurance policies with high face-values and expensive premiums. Perhaps law firms can find the needed funds by leasing less expensive office premises. A failure to find adequate funds for cybersecurity improvements not only makes law firms more vulnerable to cyber-attacks but also makes it difficult for them to comply with professional responsibility norms, thus resulting in greater legal malpractice and other risks.

**Author.** Ethan S. Burger is a legal consultant and academic who has written extensively about corporate governance, professional responsibility, Russian-related legal issues, and transnational financial crime. He has been a full-time faculty member at American University's School of International Service and the University of Wollongong's Faculty of Law.

He is an Adjunct Professor at the Institute of World Politics. Formerly, he taught at Washington College of Law, Georgetown University Law Center, and Vilnius University. He is also a member of the Association of Professional Responsibility Lawyers and the ABA Center for Professional Responsibility. Mr. Burger earned his A.B. from Harvard University and his J.D. from the Georgetown University Law Center.

The author would like to acknowledge the helpful feedback and encouragement he received from Eileen Garczynski, Ames & Gough's Senior Vice President and Partner, and George R. Clark, Member of the District of Columbia Bar Legal Ethics Committee and Director of the Association of Professional Responsibility Lawyers.

## ARTICLE CONTENTS

I.	Introduction.....	237
II.	Law Firm Work-from-Home and Returning-to-Work Policies .....	242
	A. WFH Policies.....	243
	B. RTW Policies .....	248
III.	Professional Responsibility and Legal Practice Norms During the COVID-19 Pandemic .....	252
	A. Communications .....	253
	B. Confidentiality .....	256
	C. Competence .....	259
	D. Diligence.....	261
	E. Supervising Subordinate Attorneys and Staff.....	264
	F. COVID-19 and the Unauthorized Practice of Law .....	266
	G. Rethinking Two Formal Opinions in the Pandemic .....	268
	1. Cyber Incident Awareness.....	271
	2. Incident Response Plans .....	275
	H. A Need for Law Firm Ethics Counsel in the Post-Pandemic World .....	277
IV.	COVID-19-Related Legal Malpractice.....	278
V.	Law Firm Cybersecurity.....	284
	A. Reducing Law Firm Vulnerability to Cyber-Attacks .....	289
	B. Principle vs. Rule-Based Cybersecurity .....	296
	C. Law Firm Best Cybersecurity Practices .....	298
VI.	Cyber-Insurance.....	300
VII.	Some Takeaways .....	307

## I. INTRODUCTION

The COVID-19 pandemic (the pandemic) has dramatically, and perhaps permanently, changed how most U.S. lawyers and their law firms deliver legal services.<sup>1</sup> While many lawyers have worked remotely for years, many law firms chose to increase their level of remote operations in response to the COVID-19 outbreak.

In the early stages of the pandemic, most law firms sought to conform their activities to the Centers for Disease Control and Prevention (CDC), Occupational Safety and Health Administration (OSHA), and state health authority guidelines by immediately reducing the size of gatherings, encouraging social distancing, and mandating the use of protective gear.<sup>2</sup>

---

1. For ease of understanding, this Article will use “lawyer” and “law firm” as synonyms, except when the context demands otherwise. In general, the ABA Model Rules of Professional Conduct regulate lawyers as individuals, rather than lawyers as part of law firms or other organizations. *See* Ted Schneyer, *Professional Discipline for Law Firms?*, 77 CORNELL L. REV. 1, 26–27, 45–46 (1991) (criticizing the Rules for their focus largely on the conduct of lawyers on an individualized basis as opposed to law firms); *see also* Annie Simkus, *Preventing Data Breaches at Law Firms: Adapting Proactive Management-Based Regulation to Law-Firm Technology*, 59 ARIZ. L. REV. 1111, 1115–16, 1118, 1121–22 (2017) (observing how the Model Rules call for reasonable efforts but make no reference to how law firms should use various technologies, leaving the individual attorney with the sole duty to protect the client and the client’s property). Note that this Article was prepared in 2020 before the COVID-19 vaccination was made widely available to the U.S. adult and teenage population by the Biden Administration in 2021.

According to an article from 2019, roughly three-quarters of the approximately 1.3 million lawyers licensed in the United States are in private practice, a majority of whom work in law firms of ten attorneys or less. Sally Kane, *Working in a Private Practice Law Firm*, THE BALANCE CAREERS (Jan. 12, 2019), <https://www.thebalancecareers.com/law-firm-life-2164667> [https://perma.cc/W99B-VMGX].

2. The CDC provided, and continues to provide updated, medical, and public health information to state and local governments, organizations, and individuals to allow them to plan and prepare their responses to COVID-19. The permalinks below provide the preserved version at the initial writing of this Article, whereas the preceding URLs provide the current information. The CDC is not a regulatory body and as such, its power is one of persuasion. *See Workplaces and Businesses*, CTRS. FOR DISEASE CONTROL & PREVENTION, <https://www.cdc.gov/coronavirus/2019-ncov/community/organizations/businesses-employers.html> [https://perma.cc/W57M-PJJX] (providing resources for employers, workers, essential services sectors, and specific industries to plan, prepare, and respond to COVID-19); *Holiday Tips*, CTRS. FOR DISEASE CONTROL & PREVENTION, <https://www.cdc.gov/coronavirus/2019-ncov/daily-life-coping/holidays/winter.html> [https://perma.cc/TJ49-2DFB] (“Travel may increase your chance of spreading and getting COVID-19. The CDC continues to recommend postponing travel and staying home, as this is the best way to protect yourself and others this year.”); *Government Response to Coronavirus, COVID-19*, USA.GOV, <https://www.usa.gov/coronavirus> [https://perma.cc/6X3K-T5LZ] (providing “information from federal agencies on how they’re responding to the coronavirus pandemic”); *COVID-19 Resources for State Leaders: State Reopen Plans*, COUNCIL OF STATE GOV’TS, <https://web.csg.org/covid19/state-reopen-plans> [https://perma.cc/6YUJ-EZ4N] (setting forth state-by-state policies for reopening); *State COVID-19 Data and Policy Actions*, KFF (June 3, 2021), <https://www.kff.org/coronavirus-data-and-policy/actions/>.

Furthermore, law firms cut back on in-person meetings with clients, government officials, judicial personnel, vendors, etc., by increasing the use of various forms of telecommunications, including video conferencing,<sup>3</sup> and by reducing non-essential travel.<sup>4</sup>

Most law firms operated with skeletal staffs physically coming into the office while encouraging their lawyers and non-essential staff to work from home to the extent possible.<sup>5</sup> As a result, it was expected that law firm efficiency and income would drop precipitously, with the additional costs associated with offsite operations eating into their profits. Under the circumstances, it seemed law firms would receive fewer work assignments from their clients, most of whom also faced challenging situations.<sup>6</sup> In

---

COVID-19/issue-brief/state-data-and-policy-actions-to-address-coronavirus [<https://perma.cc/S9UQ-9M38>] (providing an interactive map for each state, territory, and region of the United States to view each state's reopening plan); *COVID-19 State Reopening Guide*, MULTISTATE, <https://www.multistate.us/issues/covid-19-state-reopening-guide> [<https://perma.cc/3N5G-67XR>] (exploring data from states on COVID-19 related metrics).

3. See Ellen Rosen, *The Zoom Boom: How Videoconferencing Tools Are Changing the Legal Profession*, ABAJOURNAL (June 3, 2020, 8:00 AM), <https://www.abajournal.com/web/article/ethics-video-conferencing-tools-are-changing-the-legal-profession> [<https://perma.cc/93XP-L7LM>] (noting "there is no specific rule governing ethical obligations" concerning videoconferencing, but it must be done in a manner consistent with the requirements found in Rules 1.1 *Competence*, 1.6 *Confidentiality of Information*, and 5.1 *Responsibilities of a Partner or Supervisory Lawyer*).

4. See Lizzy McLellan & Christine Simmons, *Paul Weiss Restricts Travel, Orrick Postpones Partner Retreat Over Coronavirus Fears*, AM. LAW. (Feb. 26, 2020, 2:36 PM), <https://www.law.com/americanlawyer/2020/02/26/paul-weiss-restricts-travel-orrick-cancels-partner-retreat-over-coronavirus-fears/> [<https://perma.cc/KWN2-EQEE>] ("Major law firms are postponing or canceling events in the U.S. and further limiting international travel as the virus spreads.").

5. See Debra Cassens Weiss, *More Than 50 Law Firms Require or Allow Work from Home Because of COVID-19 Concerns*, ABAJOURNAL. (Mar. 18, 2020, 12:34 PM), <https://www.abajournal.com/news/article/more-than-50-law-firms-require-encourage-or-allow-work-at-home-because-of-covid-19-concerns> [<https://perma.cc/ZD87-TS4D>] (recognizing at the beginning of the pandemic "[t]he number of law firms requiring or encouraging work at home [was] growing larger by the day").

6. See *COVID-19: Business Impact on Law Firms*, INTAPP (Apr. 16, 2020), <https://www.intapp.com/insights/covid-19-business-impact-law-firms/> [<https://perma.cc/9DQU-MXDW>] (discussing changing and shrinking demand for legal services); GARTNER, INC., 2021 LEGAL PLANNING & BUDGETING 3 (2020), <https://emtemp.gcom.cloud/ngw/globalassets/en/legal-compliance/documents/insights/legal-state-of-the-function.pdf> [<https://perma.cc/2G6K-P6M9>] ("Legal operations teams' responsibilities are narrowing to focus on critical priorities for 2021 to manage resources and support remote work."); *Law Departments React to Pandemic Disruption*, ALTMAN WEIL, INC. (Nov. 17, 2020), <http://www.almanweil.com/CLPR20/> [<https://perma.cc/4MVF-AZTA>] (explaining COVID-19's challenges and effects on law departments thus far and the need to adjust future plans).

many cases, this situation forced many law firms to reduce their attorney and staff salaries.<sup>7</sup>

Due to the pandemic, many law firms increased their reliance on technology to manage their operations—the results were better than many expected.<sup>8</sup> Writing in the *New York Law Journal*, Charles R. Macedo of the law firm Amster, Ritherstein, & Ebenstein observed that while on first impression it might seem that COVID-19 had been an entirely disruptive force for law firms, the truth is more complex.<sup>9</sup> With the passage of time, most law firms adjusted to working in the pandemic.<sup>10</sup> Indeed, COVID-19

---

7. Many law firms have reduced the compensation of their attorneys and laid-off staff to deal with revenue shortfalls due to COVID-19. See Danielle Bruff, *Trimming the Fat: COVID-19 and a Slow Economy Have Forced Law Firms of All Sizes to Cut Costs*, A.B.A. J., Dec.–Jan. 2020–2021, at 18, 18, <https://www.abajournal.com/magazine/article/covid-19-and-a-slow-economy-have-forced-law-firm-s-of-all-sizes-to-cut-costs> [https://perma.cc/QSS5-7EYH] (“[T]here have been multiple press reports about law firms furloughing and laying off staffers and lawyers while cutting pay and implementing austerity measures.”); *Adjusting the COVID-19 Response: How Law Firms Are Altering Austerity Measures*, AM. LAW. (Dec. 28, 2020, 9:00 AM), <https://www.law.com/americanlawyer/2020/12/28/adjusting-the-covid-19-response-how-law-firms-are-altering-austerity-measures/> [https://perma.cc/NSA5-TWHT] (suggesting many law firms had to implement pay cuts and layoffs to survive the COVID-19 pandemic); *Pay Cuts, Layoffs, and More: How Law Firms Are Managing the Pandemic*, AM. LAW. (July 31, 2020, 5:00 AM), <https://www.law.com/americanlawyer/2020/07/31/pay-cuts-layoffs-and-more-how-law-firms-are-managing-the-pandemic> [https://perma.cc/TNQ5-XU6V] (“Major law firms adopted drastic measures to mitigate the economic effects of the coronavirus pandemic and recession. Some firms have rolled back their pay cuts.”). Nonlegal staff “cuts explain part of the 7.4% dip in [law firms’] general expenses, compared to growth of 5.4% in the first nine months of 2019.” Dan Packel, *Most Big Firms Are Increasing Revenue, but Performance Gap Steadily Grows*, AM. LAW. (Dec. 2, 2020, 5:13 PM), <https://www.law.com/americanlawyer/2020/12/02/most-big-firms-are-increasing-revenue-but-performance-gap-steadily-grows/> [https://perma.cc/4ZDT-WNW7].

8. See Jeffrey Lowe & Brian McMahon, *Law Firms Survived 2020 Better Than They Could Have Hoped. Now What?*, AM. LAW. (Nov. 23, 2020, 5:00 AM), <https://www.law.com/americanlawyer/2020/11/23/law-firms-survived-2020-better-than-they-could-have-hoped-now-what/> [https://perma.cc/AMR7-9CR4] (stating a majority of law firms seem to be pleased by “how [their] investment[s] in technology [have] paid off” since the start of the pandemic but recognizing that there is no substitute for in-person mentoring).

9. Charles R. Macedo, *The Impact of COVID-19 on Law Firms: Disruption, Acceleration and Innovation*, MID-MARKET REP. (June 8, 2020, 12:00 PM), <https://www.law.com/mid-market-report/2020/06/08/the-impact-of-COVID-19-on-law-firms-disruption-acceleration-and-innovation> [https://perma.cc/LSS7-RK32] (discussing how one law firm already had everything needed to work remotely, but merely had not implemented it; subsequently, the firm upgraded its systems).

10. It is important to keep in mind that the legal community is large and diverse. Consequently, how they have reacted operationally to the pandemic is necessarily varied. Furthermore, it is not clear when the pandemic will end. Tim Loh, *Fauci Says End to Pandemic Is in Sight, Thanks to Vaccines*, BLOOMBERG (Nov. 12, 2020, 7:36 AM), <https://www.bloomberg.com/news/articles/2020-11-12/covid-won-t-be-pandemic-for-long-thanks-to-vaccines-fauci-says> [https://perma.cc/LYS8-MMNZ]; Sam Meredith, *Dr. Fauci Says ‘Help Is on the Way’ with Vaccines, but Doubts Covid Can Ever Be*

has been “an accelerator of readily available, yet rarely used technologies that support social distancing, as well as, an inspiration for innovation.”<sup>11</sup> The result has been “[f]orced experimentation”,<sup>12</sup> that is, unplanned adaptive behavior.

Technological tools used by law firms for legal and administrative activities have implications for staffing needs, office space requirements,<sup>13</sup> and management or supervisory procedures. Actions taken in each of these areas gave rise to certain risks, which were by-products of the COVID-19 virus, albeit, not caused by it.

Due to the pandemic, law firms have had to address certain secondary (i.e., not health-related) risks arising from: (i) non-compliance with professional conduct norms, (ii) legal malpractice, (iii) increased cybersecurity vulnerability, and (iv) need for cyber-insurance, to wit:

- Compliance risks for failing to observe relevant rules of professional conduct in areas such as communications, competence, confidentiality, diligence, and supervision have seemingly increased. What might lawyers and their law firms have to do to improve performance in these areas?

---

Eradicated, CNBC (Nov. 12, 2020, 9:55 AM), <https://www.cnbc.com/2020/11/12/coronavirus-dr-fauci-says-he-doubts-whether-covid-can-be-eradicated.html> [<https://perma.cc/UE68-9YPZ>].

11. Macedo, *supra* note 9; see *Assessing the Impact of COVID-19 on Legal Operations*, ASHURST, <https://www.ashurst.com/en/innovation/ashurst-advance/assessing-the-impact-of-covid-19-on-legal-operations> [<https://perma.cc/G4VK-D4XA>] (explaining how COVID-19 caused law firms to adopt new technology, advance current technology, and promote innovation).

12. See Lyle Moran, *Business as [Un]Usual: Will the COVID-19 Pandemic Fundamentally Remake the Legal Industry?*, A.B.A. J., Aug.–Sept. 2020, at 34, 34–37, <https://www.abajournal.com/magazine/article/will-the-COVID-19-Pandemic-fundamentally-remake-the-legal-industry> [<https://perma.cc/E888-VK6H>] (identifying the ways the legal community needed to try existing technology to continue business through the pandemic).

13. The average law firm spends roughly “between 9 and 12% of their overhead costs on rent.” This figure will change in the future as many law firms are looking for smaller and less expensive office space options as more of their employees telecommute. See Danielle Antosz, *Law Firm Overhead: Understanding, Diagnosing, & Fixing Profit Killers*, ASKCODY (June 2, 2020, 9:15 AM), <https://www.askcody.com/blog/law-firm-overhead> [<https://perma.cc/7YNL-TQU8>] (“[U]nless you want to run a digital law firm, you have to have a place to do business.”). There may be additional cost savings as law firms “back off some of the design trends . . . such as large common areas and cafe-style lunchrooms, as social distancing requirements make those sorts of spaces problematic.” Brenda Sapino Jeffreys, *Firms Are Designing New Offices With COVID-19 in Mind*, AM. LAW. (July 7, 2020, 2:48 PM), <https://www.law.com/americanlawyer/2020/07/07/firms-are-designing-new-offices-with-covid-19-in-mind/> [<https://perma.cc/VB7D-JK82>].

- Legal malpractice risks for not following established standards for the practice of law pursuant to different theories for lawyer liability. What has been the effect of COVID-19 on legal malpractice claims? What are the lessons relating to attorney and staff oversight due to personnel changes and their impact on how lawyers and their law firms deliver legal services to their clients?
- Cybersecurity risks have grown but extant law firm cybersecurity policies, programs, and procedures generally do not reflect the magnitude of the requirements for conducting effective remote operations.<sup>14</sup> The result is that most law firms are finding they have inadequate hardware, software, procedures, and personnel to support their current profile. Their leadership is often fatalistic about their ability to protect themselves from cyber-attacks by criminals or nation-states.<sup>15</sup> Many believe efforts to improve cybersecurity will have a negative impact on efficiency and productivity.
- There may be risks arising from the failure to procure cyber-insurance. While many law firms have purchased cyber-insurance

---

14. By disrupting law firm operations, COVID-19 has made law firms more vulnerable to cyber-attacks. See *COVID-19: Working Remotely - What Attorneys Need to Know to Avoid Cyberthreats and Privacy Risks*, ABA (Mar. 30, 2020), <https://www.americanbar.org/events-cle/ecd/ondemand/398900967> [https://perma.cc/4U8C-GTBB] (describing the need for cybersecurity due to the pandemic). On a periodic basis, Marsh & McLennan issues excellent research papers on cybersecurity and cyber-insurance issues. See Jim Holtzclaw & Reid Sawyer, *Cybersecurity After COVID-19: 10 Ways to Protect Your Business and Refocus on Resilience*, MARSH, <https://coronavirus.marsh.com/us/en/insights/research-and-briefings/cybersecurity-after-covid-19.html> [https://perma.cc/WEV8-AE2E] ("The post-pandemic recovery and preparation period presents the opportunity for companies to rebuild to a new normal, with enterprise resilience as a pervasive goal."); *COVID-19: Cybersecurity Checklist for Remote Working*, MARSH, <https://coronavirus.marsh.com/us/en/insights/research-and-briefings/covid-19-cybersecurity-remote-working.html> [https://perma.cc/N3NG-6GRP] (providing an inclusive list of cybersecurity recommendations for remote working); *COVID-19: Next Steps for Your Cyber Insurance*, MARSH, <https://coronavirus.marsh.com/us/en/insights/research/covid-19-next-steps-for-cyber-insurance.html> [https://perma.cc/D2V8-3HP6] (suggesting next steps for cybersecurity including policy response and renewal preparation); see also William E. Gericke & Deborah Winokur, *Ethical Issues with Remote Work During COVID-19*, COZEN O'CONNOR (Mar. 30, 2020), <https://www.cozen.com/news-resources/publications/2020/ethical-issues-with-remote-work-during-covid-19> [https://perma.cc/LG55-P5JB] (examining certain "ethical issues employers are facing while . . . operating remotely," including those in connection with outsourcing legal services).

15. See Herb Lin, *Reflections on the SolarWinds Breach*, LAWFARE (Dec. 22, 2020, 8:01 AM), <https://www.lawfareblog.com/reflections-solarwinds-breach> [https://perma.cc/H6FZ-9FSQ] (describing the U.S. government's inability to prevent the SolarWinds hack and how it may lower expectations that private organizations, such as law firms, are capable of ensuring their cybersecurity).

policies, their efficacy is uncertain since the policies typically have significant exclusions and contain other grounds for denying coverage in the event of a claim. Rather than spend money on cyber-insurance, some people contend that a better use of the funds would be to acquire additional cybersecurity tools and adopt better cybersecurity practices.

Before examining the aforementioned secondary risks that law firms encounter as a result of COVID-19, this Article examines law firm working-from-home and returning-to-work policies during the pandemic.

## II. LAW FIRM WORK-FROM-HOME AND RETURNING-TO-WORK POLICIES

COVID-19 work-from-home (WFH) and return-to-work (RTW)<sup>16</sup> policies set the stage to examine law firm risks associated with: (i) non-compliance with professional conduct norms, (ii) legal malpractice, (iii) increased cybersecurity vulnerability, and (iv) failure to procure cyber-insurance. To successfully transition to the post-pandemic era, law firms must strive to adapt their culture with respect to their: (i) operational methods and (ii) personnel composition and roles.<sup>17</sup> The existence and

---

16. The term “RTW” is a bit of a misnomer since it includes situations where some workers continued their normal work schedule, even after the outbreak of the pandemic. See, e.g., Christine Simmons et al., *Get Comfortable at Home: Big Firms Plan to Allow Remote Work for Rest of Year*, AM. LAW. (Sept. 3, 2020, 5:00 AM), <https://www.law.com/americanlawyer/2020/09/03/get-comfortable-at-home-big-firms-plan-to-allow-remote-work-for-rest-of-year> [<https://perma.cc/J4WT-A5SK>] (noting how at Shutts & Bowen and Carlton Fields about 25% of attorneys were working in the office on an average day).

17. See Eric Farber, *Six Steps to a Better Law Firm Culture in the Age of the Digital Water Cooler*, ABA (Dec. 10, 2020), [https://www.americanbar.org/groups/gpsolo/publications/gp\\_solo/2020/november-december/six-steps-better-law-firm-culture-digital-water-cooler](https://www.americanbar.org/groups/gpsolo/publications/gp_solo/2020/november-december/six-steps-better-law-firm-culture-digital-water-cooler) [<https://perma.cc/4DMW-VZWR>] (stressing, *inter alia*, the importance of honesty, determining and following best practices, staying true to organizational values, and checking in with, not checking on people (i.e., avoiding micromanaging)); Teresa Matich, *How to Challenge Norms and Build a Strong Law Firm Culture*, CLIO (Apr. 30, 2021), <https://www.clio.com/blog/law-firm-culture> [<https://perma.cc/XB28-33XU>] (providing a handbook on law firm culture); see also Peter Roberts, *Compensation, Motivation, and the Social Contract*, LAW PRAC. TODAY (July 14, 2015), <https://www.lawpracticetoday.org/article/compensation-motivation-and-the-social-contract/> [<https://perma.cc/RTH2-HM6Q>] (discussing social contracts connected to law firm practice: with the client, paying the staff, paying the attorneys, paying the partners, paying of counsel, during bad times); Jordan Rothman, *Law Firms Should Be Shamed for Reopening Offices Too Soon*, ABOVE THE L. (Dec. 2, 2020, 11:19 AM), <https://abovethelaw.com/2020/12/law-firms-should-be-shamed-for-reopening-offices-too-soon/> [<https://perma.cc/C4MV-B6LU>] (providing an example of law firms violating a social contract by encouraging workers to risk their health and safety).

nature of trust is a critical element in law firm culture; its role is considered in the analysis below.<sup>18</sup>

#### A. WFH Policies

For most law firms, COVID-19 led to a drop in the demand for their legal services. While figures vary widely, the overall decline has been estimated to be in the 20–30% range.<sup>19</sup> With revenues down, law firms had to consider whether to cut law firm salaries as well as partners' draws. Furthermore, law firms had to undertake other cost-cutting measures. On an interim basis, the extent of these cuts might be reduced with funds from government programs, but the availability of such funds is limited.<sup>20</sup> Reductions in salaries may not be sufficient to cover the shortfall, making it necessary to terminate personnel, including requiring some partners to leave the firm. In many respects, this is a zero-sum game pitting the interests of some lawyers against staff, some staff members against other staff members, and some lawyers against other lawyers.<sup>21</sup> This situation can be devastating

---

18. See Roberts, *supra* note 17 (discussing the necessity of honoring the social contract in difficult financial times).

19. Daniel S. Wittenberg, *The Pandemic's Dramatic Effect on the Business of Law*, ABA (Oct. 28, 2020), <https://www.americanbar.org/groups/litigation/publications/litigation-news/business-litigation/the-pandemics-dramatic-effect-the-business-law> [https://perma.cc/8ZL4-2KPM].

20. See *Paycheck Protection Program*, U.S. SMALL BUS. ADMIN., <https://www.sba.gov/funding-programs/loans/coronavirus-relief-options/paycheck-protection-program> [https://perma.cc/5BVG-HR6C] (providing in early 2021: “The Paycheck Protection Program (PPP) provides loans to help businesses keep their workforce employed during the Coronavirus (COVID-19) crisis.”); Dylan Jackson, *Big Law Firms Got Millions of Dollars to Preserve Payroll. Some Made Cuts Anyway*, AM. LAW. (July 7, 2020, 6:40 PM), <https://www.law.com/americanlawyer/2020/07/07/big-law-firms-got-millions-of-dollars-to-preserve-payroll-some-made-cuts-anyway/> [https://perma.cc/RGL8-FMSR] (“In all, at least 47 Am Law 200 firms received PPP loans through the SBA as part of a stimulus program that allotted \$350 billion in March [2020] to stem the rising tide of unemployment catalyzed by the coronavirus pandemic. Those loans totaled between \$218 million and \$445 million, according to data released by the SBA.”); Debra Cassens Weiss, *Many Law Firms That Applied for Paycheck Protection Loans Are Still Waiting; Texas Lawyer Sues*, ABAJOURNAL (Apr. 29, 2020, 12:45 PM), <https://www.abajournal.com/news/article/many-law-firms-that-applied-for-paycheck-protect-ion-loans-are-still-waiting-texas-lawyer-sues> [https://perma.cc/AR9J-4LCJ] (stating, in April 2020, many firms have applied for small business loans, and many have yet to receive those loans); Reece Guida, *What Is the CARES Act and How Can It Help Legal Professionals?*, NATL L. REV. (Apr. 14, 2020), <https://www.natlawreview.com/article/what-cares-act-and-how-can-it-help-legal-professionals> [https://perma.cc/GD7J-26Q4] (“Attorneys who own their own practice can take advantage of the 2020 CARES Act to protect their business and employees during the economic downturn brought on by COVID-19.”).

21. See Douglas R. Richmond, *Professional Responsibilities of Law Firm Associates*, 45 BRANDEIS L.J. 199, 224–33 (2007) (discussing associate-partner billable hour issues, where an associate has billed time to a client that a partner is reluctant to pass on to the client).

to law firm morale.<sup>22</sup> Nonetheless, it is worth noting that a June 2020 survey of a small sample of lawyers and law firm staff indicated that they “enjoy working remotely so much that 67% want to continue that arrangement once offices fully reopen following the coronavirus pandemic[,]” suggesting that it may be too early to make reliable generalizations about lawyers’ attitudes about working from home.<sup>23</sup>

To respond to the pandemic, the first order of business was deciding who must go into the office for work, what work would they do while onsite, and what social distancing rules to observe. It soon became apparent that a large share of the work performed in traditional office space can be accomplished remotely.<sup>24</sup> Software developed to support law firm remote operations facilitated this process.<sup>25</sup> As a result, a large share of law firm personnel need not go to work every day. Law firms set up systems using staggered hours. Onsite personnel were expected to observe social distancing rules, as set out in law firm RTW policies.

A great deal of support staff work involves using specialized communication systems, computers, copiers, scanners, etc., located in law

---

22. See Andrew Maloney, *Concerns Over Burnout and Retention Arise, Even as Firms Improve Collaboration*, AM. LAW. (Sept. 23, 2020, 6:33 PM), <https://www.law.com/americanlawyer/2020/09/23/concerns-over-burnout-and-retention-arise-even-as-firms-improve-collaboration> [<https://perma.cc/M9FA-5DNF>] (explaining law firm morale can remain low even with improvement in efficiency and profitability); see also Pam Smith, *Law Firm Leaders Report Lower Morale and Now Expect Longer COVID-19 Impacts*, INTAPP (Apr. 27, 2020), [https://www.intapp.com/blog\\_posts/law-firm-leaders-report-lower-morale-longer-covid-19-impacts](https://www.intapp.com/blog_posts/law-firm-leaders-report-lower-morale-longer-covid-19-impacts) [<https://perma.cc/DS5D-WZUD>] (noting a survey indicated “[n]early two-thirds of firms report[ed] lowered employee morale as one of the significant consequences of the pandemic”); Mike Short et al., *Covid-19 Recovery Playbook: Managing a Law Firm in the First Phase of the Crisis*, AM. LAW. (Apr. 6, 2020, 4:10 PM), <https://www.law.com/americanlawyer/2020/04/06/covid-19-recovery-playbook-managing-a-law-firm-in-the-first-phase-of-the-crisis> [<https://perma.cc/SLM2-BEYG>] (urging law firm management to monitor morale and well-being of law firm personnel).

23. See Brenda Sapino Jeffreys, *Legal Professionals Want to Keep Working from Home, but Will That Last?*, AM. LAW. (June 11, 2020, 4:36 PM), <https://www.law.com/americanlawyer/2020/06/11/legal-professionals-want-to-keep-working-from-home-but-will-that-last/> [<https://perma.cc/PFK8-8XHN>] (indicating 92% of those surveyed believed their clients were satisfied with arrangements to work and meet remotely).

24. Teresa Matich, *The Complete Guide to Working Remotely as a Lawyer*, CLIO 3–4, <https://www.clio.com/guides/complete-guide-lawyers-remote-work> [<https://perma.cc/6P3Z-ZAUE>] [hereinafter Matich, *Complete Guide to Working Remotely*].

25. See *Law Practice Management Software Made Easy*, PRACTICEPANTHER, <https://www.practicepanther.com/> [<https://perma.cc/79NM-G44T>] (explaining the benefits of the software product); *What Practice Management Software Connects Everyone at Your Firm?*, THOMSON REUTERS, <https://legal.thomsonreuters.com/en/c/elite-pro-law-one-office-now?> [<https://perma.cc/G455-Z249>] (“Serve clients anywhere with secure, on-the-go access to critical files.”).

firm office space; in turn, only a limited share of such work can be performed remotely.<sup>26</sup> Law firms had the option of moving their equipment offsite where the risk of exposure to the virus was limited and obtaining tech support was feasible. In any event, a dilemma arose—persons who could not do their jobs remotely or find a safer location to complete their tasks had to go into the office, find new tasks to perform (possibly involving retraining), or face the risk of being deemed redundant.<sup>27</sup>

The transition from onsite to offsite work is not always a seamless process. Another complicating fact is neither lawyers nor clients want to perform tasks traditionally considered to be administrative or secretarial.<sup>28</sup> Of course, if lawyers fear that staff members cannot properly complete tasks on time, lawyers will be tempted to delegate these tasks to others, including other staff members, subordinate lawyers, or complete the tasks themselves; in the latter two situations, this may present a billing or revenue problem.

Over time, most law firms seem to have gotten a better sense of what work can be performed remotely and the best way to accomplish it.<sup>29</sup>

---

26. See *Support Staff Structures for the Law Firm of the Future*, WILLIAMS LEA (Aug. 28, 2020), <https://www.williamslea.com/blog/support-staff-structures-for-the-law-firm-of-the-future> [https://perma.cc/AVA7-UB6K] (“The consensus is clear: The COVID-19 crisis is accelerating new ways of working and accentuating the need for firms to better understand how, and how much support, their secretarial teams are able to provide when working remotely.”).

27. See Doug Austin, *As the Pandemic Continues, Lawyer and IT Jobs May Still Be Fine. Support Staff? Maybe Not: Legal Jobs Trends*, EDISCOVERY TODAY (Dec. 1, 2020), <https://ediscoverytoday.com/2020/12/01/as-the-pandemic-continues-lawyer-and-it-jobs-may-still-be-fine-support-staff-maybe-not-legal-jobs-trends/> [https://perma.cc/9KZF-3JMJ] (stating many non-attorney-related jobs will be permanently reduced after the pandemic); Dan Roe, *As Firms Restructure Staffs for the Post-Pandemic Future, Who Will Be Protected and Exposed?*, AM. LAW. (Nov. 29, 2020, 9:22 AM), <https://www.law.com/americanlawyer/2020/11/29/as-firms-restructure-staffs-for-the-post-pandemic-future-who-will-be-protected-and-exposed> [https://perma.cc/G52C-HJPD] (explaining the pandemic caused layoffs in legal services and staff in law firms across the country); Patrick Smith, *'The Last Straw': The Pandemic Is Accelerating Known Need to Cut Admins*, AM. LAW. (July 29, 2020, 7:50 PM), <https://www.law.com/americanlawyer/2020/07/29/the-last-straw-the-pandemic-is-accelerating-known-need-to-cut-admins> [https://perma.cc/3LYQ-N8CB] (weighing in on the fact that employment in the legal landscape will change as a result of the pandemic).

28. See *How Is the Role of Legal Support Staff Changing?*, ONE LEGAL (Apr. 20, 2017), <https://www.onelegal.com/blog/how-is-the-role-of-legal-support-staff-changing/> [https://perma.cc/Q2W5-XJWC] (“But thanks to the advent of technology, the role of legal support staff is in an almost constant state of flux, with job responsibilities that often overlap and have changed significantly in the last decade or two.”).

29. See Jenn Betts, *Legal Collaboration Technology: Opportunities and Challenges*, LEGAL INTELLIGENCER (Oct. 1, 2020, 1:06 PM), <https://www.law.com/thelegalintelligencer/2020/10/01/legal-collaboration-technology-opportunities-and-challenges/> [https://perma.cc/AE84-7RXP]

Remote work demands the ability to work collaboratively, but not all law firms, lawyers, and staff can develop the ability to collaborate online effectively.<sup>30</sup> Law firm management is more likely to be inclined to train lawyers than staff because lawyers are more difficult to replace, and their termination is more likely to have a severe impact on law firm morale.

Trust is critical to the success of any law firm. The issue of trust presents itself in many forms and different contexts. It is necessary to consider trust between supervisor and subordinate, trust among colleagues at the same level of responsibility, trust between persons at different levels, and trust between law firm personnel and law firm clients.<sup>31</sup> Trust can involve belief (or faith) in another person's skills (ability to perform a task) or when relating to communications (thoroughness, honesty, or accuracy). Familiarity makes it easier to establish trust in another person. The absence or loss of trust, in particular involving people who lack a prior history of working together, either in person or remotely, can be difficult to establish or re-establish.

Once law firms ceased to work from their offices, they needed to develop new parameters to measure the effectiveness of their personnel operations. While such criteria may be appropriate for support staff functions, they cannot be easily used for the performance of legal work, as greater discretion and judgment are generally involved. Was it realistic to assign a person (or group of persons) a task to complete within a set amount of time? When did the person in question start the particular task? At the time the task was

---

(discussing, *inter alia*, the need to establish rules for online communication to avoid certain problems such as not following their normal protocols designed to protect privilege and confidentiality). See generally DENNIS M. KENNEDY & THOMAS L. MIGHELL, THE LAWYER'S GUIDE TO COLLABORATION TOOLS AND TECHNOLOGIES: SMART WAYS TO WORK TOGETHER 6–8 (2d ed. 2018) (covering topics such as (i) collaborating within your firm and outside your firm, (ii) online and offline collaboration on documents, (iii) managing cases and transactions, (iv) tools to use, (v) collaboration platforms, (vi) collaboration strategy development, (vii) practical issues and techniques, and (viii) the future use of collaborating in the legal practice).

30. See, e.g., Alison Doyle, *What Are Collaboration Skills?*, BALANCE CAREERS (June 26, 2020), <https://www.thebalancecareers.com/collaboration-skills-with-examples-2059686> [<https://perma.cc/4KR7-FMDC>] (“Collaboration skills enable you to successfully work toward a common goal with others. They include communicating clearly, actively listening to others, taking responsibility for mistakes, and respecting the diversity of your colleagues.”).

31. See Jeremy Byellin, *Five Tips for Building Trust with Clients*, THOMSON REUTERS, <https://legal.thomsonreuters.com/en/insights/articles/five-tips-for-building-trust-with-clients> [<https://perma.cc/RK89-NED4>] (providing advice on how to build trust with clients); Richard B. Cohen, *8 Tips to Get Your Boss to Trust You*, ABOVE THE L. (Oct. 13, 2017, 6:59 PM), <https://abovethelaw.com/2017/10/8-tips-to-get-your-boss-to-trust-you> [<https://perma.cc/4D6W-MPW4>] (offering suggestions for associates or staff to help establish a “culture of trust” in the workplace).

assigned, was there an adequate amount of time to complete the task properly? Was the task properly performed? Was the task accomplished in a reasonable amount of time? If any issues arose that delayed the successful completion of the task, was the appropriate supervisor notified? Is the activity one which is typically billable to a client? If so, was it billed to and collected from the client?

Remote work poses special challenges to law firm personnel. Considerable care needs to be paid to coordinating work and scheduling meetings. In general, people who developed personal relationships over time are less likely to have difficulty collaborating online. There is a considerable amount of online collaborative software now available for lawyers. Today, lawyers have numerous options for conducting video calls using iPhones or Android cellphones.<sup>32</sup> There are also communications options, in particular for video conferencing.<sup>33</sup> In either case, lawyers need to take appropriate steps to ensure they have adequate security for their communications to ensure their confidentiality.<sup>34</sup>

Given the dramatic increase in online collaboration, it is important that lawyers and their law firm staff improve their skills with the tools available to them.<sup>35</sup> There is a significant difference between having basic skills with online collaborative tools and having confidence in using them with colleagues, clients, and third parties. Since not everyone will have the same level of competence and ease with a particular system, it is inevitable that

---

32. See Jignesh, *Best Video Chat Apps for iPad and iPhone in 2021*, iGEEKSBLOG (Apr. 19, 2021), <https://www.igeeksblog.com/best-video-chat-apps-for-ipad-iphone/> [https://perma.cc/72KM-JK8T] (reviewing options for video chat apps, including WhatsApp, Facebook Messenger, Skype, and more); Abhilekh Das, *10 Best Android Video Chat Apps For 2021 | Free Video Calling Apps*, FOSSBYTES (Dec. 30, 2020), <https://fossbytes.com/best-android-video-chat-apps-video-calling/> [https://perma.cc/QDH9-678L] (“Here, we have compiled some of the best video calling apps that you can try out on your Android phone.”).

33. See Sharon Miki, *Video Conferencing for Lawyers: How to Video Conference Like a Pro*, CLIO (Mar. 16, 2021), <https://www.clio.com/blog/video-conferencing-for-lawyers/> [https://perma.cc/J32B-V7TU] (discussing Legaler, Zoom, GoToMeeting, and Webex, along with a step-by-step description of how to prepare for a meeting).

34. See Gina M. Vitiello & Chamberlain Hrdlicka, *Video Conferencing and Recording: Know the Risks Before You Connect*, LEGALTECH NEWS (Apr. 23, 2020, 10:00 AM), <https://www.law.com/legaltech/news/2020/04/23/video-conferencing-and-recording-know-the-risks-before-you-connect> [https://perma.cc/R94T-W2N2] (discussing “confidentiality, discovery and security issues”).

35. Jill Duffy, *The Best Online Collaboration Software for 2021*, PC (May 25, 2021), <https://www.pcmag.com/picks/the-best-online-collaboration-software> [https://perma.cc/YDS9-9N9G] (reviewing “[t]he best online collaboration tools”).

some people will be at a disadvantage when using them when compared to prior working arrangements.

There are usually good software training materials,<sup>36</sup> alternatively, some people need to work with a trainer individually or in a class, but even after several sessions, they may not feel comfortable making or fielding calls online. They may have difficulty picking up other people's social cues or body language, have speech patterns or accents that are difficult for some people to understand, and make gestures that might confuse others. These factors introduce a possibility for miscommunication, which can have significant consequences.

Working remotely involves more preparation than does in-person interactions. It is not always possible to readily share online non-digitalized information such as documents or reference materials. Also, for technical or security reasons, it may not be possible to bring additional people into a meeting after it has begun.

#### B. RTW Policies

In addition, RTW policies must be examined to understand law firm secondary risks. Congress created the “Occupational Safety and Health Administration (OSHA) to ensure safe and healthful working conditions . . . by setting and enforcing standards and by providing training, outreach, education and assistance.”<sup>37</sup> Early in the pandemic, OSHA issued detailed advisory guidance (i.e., recommendations) to serve as the basis for RTW policies, requiring employers to undertake:

- **Hazard Assessment[s]:** Risks of exposure to COVID-19 in the workplace are addressed through completion of a documented hazard assessment and implementation of corresponding controls, such as engineering controls (e.g., physical barriers), administrative controls (e.g., staggered shifts, health screening, workplace policies),

---

36. See, e.g., Matich, *Complete Guide to Working Remotely*, *supra* note 24, at 9, 11–12 (setting forth guidelines for remote working, such as planning for meetings by video, enacting a clear remote work policy, and tracking firm productivity).

37. *About OSHA*, U.S. DEP'T OF LAB., <https://www.osha.gov/aboutosha> [<https://perma.cc/KKL9-ZLDD>]. See *OSH Act of 1970*, U.S. DEP'T OF LAB., <https://www.osha.gov/laws-regulations/oshaact/section5-duties> [<https://perma.cc/4VJC-73CZ>] (requiring employers to “furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm”) *Regulations*, U.S. DEP'T OF LAB., <https://www.osha.gov/coronavirus/standards> [<https://perma.cc/Q9Y3-DTR3>] (quoting the General Duty Clause of the OSH Act of 1970).

and, when applicable, use of personal protective equipment (“PPE”).

- **Use of Preventive Controls:** Risks of exposure to COVID-19 and spread of the disease are prevented and minimized through good hygiene (e.g., hand hygiene, respiratory etiquette, and protocols around cleaning and disinfection), social distancing, and immediate identification and removal of sick individuals from the workplace.
- **Policies and Procedures:** Effective policies and procedures are in place to minimize employees’ exposure risks, such as procedures for prompt injury and illness reporting, remote work, sick leave, and workplace flexibility.
- **Employee Training:** Employees are trained on potential workplace exposures to COVID-19 and how to prevent the spread of COVID-19 at work, including risks of exposure to COVID-19, the employer’s COVID-19 related policies and procedures, and safe work practices (e.g., use of cloth face coverings, good hygiene practices, and cleaning and disinfection measures).<sup>38</sup>

Apparently, given the complexity of developing RTW policies and the urgency of the health care crisis, OSHA opted to issue informal guidance instead of engaging in formal rulemaking to avoid potential procedural

---

38. Chris D. Schlag, *New OSHA Guidance for Businesses Returning to Work*, OSHA L. BLOG (June 22, 2020), <https://www.oshalawblog.com/2020/06/articles/new-osha-guidance-for-business-es-returning-to-work/> [https://perma.cc/Z38Y-K2AK]; see OCCUPATIONAL SAFETY & HEALTH ADMIN., U.S. DEPT OF LAB., GUIDANCE ON PREPARING WORKPLACES FOR COVID-19 7–14 (2020), [https://www.osha.gov/sites/default/files/publications/OSHA3990.pdf?hss\\_channel=tw-92064349](https://www.osha.gov/sites/default/files/publications/OSHA3990.pdf?hss_channel=tw-92064349) [https://perma.cc/M59W-KD4J] (providing a plan to respond to COVID-19); see also NATHANIEL L. WADE & MARA G. ASPINALL, ASU COLL. OF HEALTH SOLS., ARIZ. STATE UNIV., FACING UNCERTAINTY: THE CHALLENGES OF COVID-19 IN THE WORKPLACE 12, 16 (Nov. 2020), [https://www.rockefellerfoundation.org/wpcontent/uploads/2020/11/ASU\\_Workplace\\_Commons\\_Nov2020\\_FINAL.pdf](https://www.rockefellerfoundation.org/wpcontent/uploads/2020/11/ASU_Workplace_Commons_Nov2020_FINAL.pdf) [https://perma.cc/J58A-CMQM] (“U.S. employers indicated that they are enabling employees to more easily practice good hygiene, increasing frequency of cleaning and sanitation, providing PPE including face coverings and face shields, investing in ways to increase the ability of employees to work from home, encouraging physical distancing with visual reminders and signage in buildings and allowing non-essential workers to work remotely.”); *COVID-19 Return to Work Checklist for Employers*, GUARDIAN, <https://www.guardianlife.com/coronavirus/return-to-work-checklist> [https://perma.cc/89YZ-MH25] (containing a checklist covering critical topics to consider when planning to allow workers to return to work such as: “General considerations for reopening”; “Protect vulnerable or ill employees”; “Implement exposure-reducing measures”; “Preparing facilities for social distancing”; “Employee health screening and monitoring”; and “Monitoring risk, staff absences”).

hurdles.<sup>39</sup> Based on CDC<sup>40</sup> and OSHA guidelines, several organizations developed and made available free-of-charge RTW action plans, alerts, or policies that can be adapted for law firm use;<sup>41</sup> arguably, the best one was developed by Stinson LLP.<sup>42</sup>

---

39. See *Law and Regulations*, U.S. DEPT OF LAB., <https://www.osha.gov/laws-regulations> [<https://perma.cc/9RBE-3387>] (“OSHA’s mission is to ensure that employees work in a safe and healthful environment by setting and enforcing standards, and by providing training, outreach, education and assistance. Employers must comply with all applicable OSHA standards. They must also comply with the General Duty Clause of the OSH Act, which requires employers to keep their workplace free of serious recognized hazards.”) (emphasis omitted)); Richard Fairfax, *OSHA’s Rulemaking Process: Why Does it Take So Long?*, ORCHSE, <https://www.orchse-strategies.com/orc-hse-blog/oshas-rulemaking-process-why-does-it-take-so-long/> [<https://perma.cc/PMF2-RFFQ>] (describing generally the legislative, statutory, judicial, and administrative requirements involved in the standards development process); OCCUPATIONAL SAFETY & HEALTH ADMIN., U.S. DEPT OF LAB., THE OSHA RULEMAKING PROCESS 1 (Oct. 15, 2012), [https://www.osha.gov/OSHA\\_FlowChart.pdf](https://www.osha.gov/OSHA_FlowChart.pdf) [<https://perma.cc/742P-NKX7>] (showing, through schematics, the rulemaking process can last years).

40. *Guidance for Unvaccinated People: Returning to Work*, CTRS. FOR DISEASE CONTROL & PREVENTION (June 11, 2021), <https://www.cdc.gov/coronavirus/2019-ncov/daily-life-coping/returning-to-work.html> [<https://perma.cc/6LB7-8TQR>].

41. See *COVID-19 Return to Workplace Resource Guide*, COVINGTON (Dec. 2020), <https://www.cov.com/en/news-and-insights/insights/2020/05/return-to-workplace-resource-guide> [<https://perma.cc/8HRD-RX3D>] (“As businesses across multiple industries and geographies prepare for reopening following COVID-19 closures, Covington is providing practical resources and guidance on the broad array of issues companies face as employees return to the workplace.”); Christine Gantt-Sorenson, *COVID-19: Recommendations for Return to Work and Continued Business Operations*, HAYNSWORTH SINKLER BOYD (May 15, 2020), <https://www.hbslawfirm.com/connect/blog/2020/covid-19-recommendations-for-return-to-work> [<https://perma.cc/N93N-EDET>] (summarizing “guidance issued by OSHA and the CDC, the two authoritative agencies charged with addressing workplace safety”); Brian Thiessen et al., *The Employer’s COVID-19 Workplace Playbook*, OSLER (Dec. 9, 2020), <https://www.osler.com/en/resources/regulations/2020/the-employer-s-covid-19-workplace-playbook> [<https://perma.cc/CQ9A-TAR9>] (“Having a rational and documented plan in place for making such decisions will be necessary to reduce uncertainty and ensure a safe work environment. This guide outlines the key considerations for employers in putting together such plans.”); Liz C. Watson et al., *Strategies for Developing a Return to Work Action Plan*, SEYFARTH (Apr. 17, 2020), <https://www.seyfarth.com/news-insights/strategies-for-developing-a-return-to-work-action-plan.html> [<https://perma.cc/B4VV-GGS3>] (providing “a list of some of the key issues employers will want to consider when developing a Return to Work Action Plan”); *Re-Opening After COVID-19: A Tall Order for Law Firms*, ESQUIRE DEPOSITION SOLS. (June 10, 2020), <https://www.esquiresolutions.com/reopening-after-covid-19/> [<https://perma.cc/4XYE-735M>] (“Reopening law firms must account for federal, state, and in some cases, local laws—a patchwork of new and pre-existing measures—when formulating a plan for returning their staff to office premises.”); *Providing Extensive Employer Policies for Maintaining a Vital Workforce and Worksites During COVID-19*, HUSCH BLACKWELL, <https://www.huschblackwell.com/return-to-work-policy-generator> [<https://perma.cc/5PZF-GR3Q>] (providing a tool for generating a *sui generis* plan).

42. Johnny Wang et al., *Return-to-Work Best Practices During the COVID-19 Pandemic*, STINSON (Apr. 30, 2020), <https://www.stinson.com/newsroom-publications-Return-to-Work-Best-Practices>.

Law firms will almost certainly want to have RTW policy manuals. Perhaps the best way to approach this task is to revise an existing law firm handbook to reflect current conditions.<sup>43</sup> The failure of law firms to adopt and implement operations consistent with their hazard assessments, use of preventive controls, health policies and procedures, and employee training requirements will jeopardize the health of their personnel and ability to serve their clients, as well as expose them to potential legal liability.<sup>44</sup>

---

During-the-COVID-19-Pandemic [<https://perma.cc/2EMD-F5KT>]. Stinson identifies six minimum measures an organization should undertake to generate a thorough RTW policy; together they served as headings for their RTW recommendations:

1. Create an Infectious Disease Preparedness and Response Plan
2. Conduct a Hazard Assessment for new protocols/equipment put in place consistent with OSHA rules
3. Create or update existing policies on issues impacted by COVID-19 and RTW issues, such as remote work, leave of absence and travel policies
4. Craft communications to returning workers ensuring that they are aware of the safety measures in place and how to comply with them
5. Ensure that proper personal protective equipment (PPE) (if needed) and general cleaning materials such as soap and hand sanitizer are available
6. Designate who within the company will be a resource for RTW questions

*Id.* In addition, Stinson provided a detailed best practices list falling within the scope of each of the above headings. *Id.*

43. See Kellie Pantekoeck, *How to Update Your Employee Handbook for COVID-19*, FINDLAW (June 18, 2020), <https://www.findlaw.com/smallbusiness/employment-law-and-human-resources/how-to-update-your-employee-handbook-for-covid-19.html> [<https://perma.cc/VLA9-5LFPI>] (highlighting the COVID-19 crisis as a good time to update employee handbooks); *The Complete Guide to Updating Your Employee Handbook for COVID-19*, GUSTO | BLOG (July 17, 2020), <https://gusto.com/blog/people-management/update-employee-handbook-covid19-guidelines> [<https://perma.cc/GQL7-A7H2>] (listing items to be added to a new company handbook after COVID-19); Carolyn Kick, *How to Create a COVID-19 Addendum for Your Employee Handbook*, LAUNCHWAYS (Apr. 9, 2020), <https://www.launchways.com/covid-employee-handbook-update/> [<https://perma.cc/6B8GLN8L>] (proposing adding an appendix to an existing handbook rather than creating a new document from scratch).

44. See Abbas Poorhashemi, *Impacts of the Coronavirus COVID-19 on Legal Professionals*, L. TECH. TODAY (Sept. 24, 2020), <https://www.lawtechnologytoday.org/2020/09/impacts-of-the-coronavirus-covid-19-on-legal-professionals/> [<https://perma.cc/Q4HQ-TFTU>] (mentioning some of the consequences of COVID-19 on the practice of law such as “closures of law firms, the slowdown in services, absence of clients, cancellation of appointments and agreements by clients, decrease in the available workforce due to illness or isolation and difficulty to holding specific meetings and services”).

### III. PROFESSIONAL RESPONSIBILITY AND LEGAL PRACTICE NORMS DURING THE COVID-19 PANDEMIC

Just as natural disasters do not terminate the ethical obligations of lawyers and their law firms to observe the Model Rules of Professional Conduct (the Rules), the pandemic does not release them either.<sup>45</sup> When people are under stress, they are more likely to make errors in judgment.<sup>46</sup> They are

---

45. The ABA Standing Committee on Ethics and Professional Responsibility's formal and informal ethics opinions are of great help in interpreting how the Rules are to be applied. The Model Rules consist of rules and commentary and are available online. *Model Rules of Professional Conduct*, ABA, [https://www.americanbar.org/groups/professional\\_responsibility/publications/model\\_rules\\_of\\_professional\\_conduct/](https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/) [<https://perma.cc/62H9-YYZP>]. The fifty states and the District of Columbia have their own rules based largely on those of the ABA. See *Additional Legal Ethics and Professional Responsibility Resources*, ABA, [https://www.americanbar.org/groups/professional\\_responsibility/resources/links\\_of\\_interest/](https://www.americanbar.org/groups/professional_responsibility/resources/links_of_interest/) [<https://perma.cc/YPA4-R6NG>] (listing the various rules).

In their opinions, courts in these jurisdictions often cite the ABA Formal Opinions, the American Law Institute's Restatement of Law Governing Lawyers, and other relevant materials when resolving matters of legal ethics and professional responsibility. See RONALD D. ROTUNDA & JOHN S. DZIENKOWSKI, *LEGAL ETHICS: THE LAWYER'S DESKBOOK ON PROFESSIONAL RESPONSIBILITY* § 1.2-4(a), § 1.2-4(a) n.4 (2018) (discussing ABA Formal Opinion 98-412, issued on September 9, 1998, which notes that lawyers must notify the court if their clients violate court orders prohibiting or limiting the transfer of certain property); see also *Ethics and Professional Responsibility*, GA. STATE UNIV. L. LIBR., <https://libguides.law.gsu.edu/c.php?g=253396&p=1689859> [<https://perma.cc/RYS3-QAA5>] (listing resources for codes of professional responsibility); ABA Comm. on Ethics & Pro. Resp., Formal Op. 482, at 1 (2018) (stating “[e]xtreme weather events such as hurricanes, floods, tornadoes, and fires” do not change the ethical obligations governing lawyers’ conduct); Margaret Monihan Toohey, *Five Pointers for Practicing in a Pandemic*, ABA (Apr. 8, 2020), <https://www.americanbar.org/groups/litigation/committees/ethics-professionalism/articles/2020/five-pointers-for-practicing-in-a-pandemic/> [<https://perma.cc/4543-EZRD>] (construing ABA Formal Opinion 482, which discusses legal ethics in the time of coronavirus, in particular, the danger of being deemed to be practicing law in a jurisdiction where one is not admitted). See generally VINCENT R. JOHNSON & SUSAN SAAB FORTNEY, *A CONCISE RESTATEMENT OF THE LAW GOVERNING LAWYERS* (2007) (discussing various legal ethics issues).

46. See Fun Man Fung & Chng Wei Heng, *COVID-19: How to Deal With Our Cognitive Biases*, THE CONVERSATION (June 29, 2020, 4:09 AM), <https://theconversation.com/covid-19-how-to-deal-with-our-cognitive-biases-140467> [<https://perma.cc/MD3J-7N7Z>] (“Cognitive biases often lead us to irrational behaviours . . .”); see also *Tips to Help Stressed-Out Lawyers During COVID-19 Pandemic*, ABA (May 2020), <https://www.americanbar.org/news/abanews/publications/youraba/2020/youraba-may-2020/tips-to-help-stressed-lawyers/> [<https://perma.cc/6YA5-BGH8>] (noting the prolonged impact of stress on the body); *Coping with Stress*, CTRS. FOR DISEASE CONTROL & PREVENTION (Jan. 22, 2021), <https://www.cdc.gov/coronavirus/2019-ncov/daily-life-coping/managing-stress-anxiety.html> [<https://perma.cc/P7EZ-WB2D>] (providing ways to cope with stress); Shawn Singh, *Workplace Stress and Anxiety After COVID-19*, BUSINESS.COM (Sept. 11, 2020), <https://www.business.com/articles/workplace-stress-anxiety-covid-19/> [<https://perma.cc/BV6D-G4NG>] (listing the types of activities persons do because of increased COVID-19 stress); *Mental Well-Being Resources for Lawyers During COVID-19*, HINSHAW (Mar. 23, 2020), <https://www.hinshawlaw.com/mental-well-being-resources-for-lawyers-during-covid-19>.

also likely to be less meticulous in following the dictates of the Rules, particularly when the normal routines within the law firm cannot be followed. This Section considers what lawyers need to do to ensure that their conduct is consistent with the Rules and other relevant norms for the practice of law when the conditions within the law firm are less stable due to the pandemic.

#### A. *Communications*

If the Rules were to have a hierarchy of importance, Rule 1.4 (Communications) would probably occupy the top position. With respect to communications with their clients, lawyers are expected to act “reasonably.”<sup>47</sup> In practice, this can be understood to mean that, at least initially, it is probably unrealistic to judge lawyers by their ability to communicate by pre-pandemic standards. Clients may be under considerable stress because of COVID-19. Lawyers should reach out to their clients since they may have more of a need to communicate than typically was the case, particularly about court and administrative filing deadlines.<sup>48</sup>

Rather than “discover” that lawyers cannot communicate or collaborate with their clients, they should organize client training sessions explaining the communications systems and procedures that will be used. If in-person meetings must be held, lawyers should seek to locate facilities where social distancing is possible and adequately ventilated to minimize health risks. If lawyers sense their clients cannot master the full capabilities of the communications technology available, they should consider sending documents in hard copy in advance of telephone conversations or other means of communications.

Since law firms are so dependent on information technology, it stands to reason that they would have contingency plans in the event of system failures. While cyber-attacks are probably the principal rationale for developing communication contingency plans, there are other scenarios that give rise to the need for such plans, such as fires and water damage. It is

---

hinshawlaw.com/newsroom-newsletters-335.html [<https://perma.cc/5LK4-59B3>] (providing a collection of resources for managing or addressing COVID-19 related stress).

47. MODEL RULES OF PROF'L CONDUCT R. 1.4 (AM. BAR ASS'N 2020).

48. See generally Sean Ginty & Tracy L. Kepler, *Best Practices for Law Firms During a Pandemic*, THE GEN. AGENCY, INC., <https://www.generalagencyinc.com/wp-content/uploads/sites/86/2020/04/Best-Practices-for-law-Firms-During-a-Pandemic.pdf> [<https://perma.cc/JT4N-VXHP>] (providing suggestions for law firms during COVID-19).

possible that these scenarios anticipate the need to work remotely since, in the event of damage to law firms' main offices, operating in other locations is foreseeable.

Ideally, contingency plans anticipate working with reduced staff, forwarding electronic voice messages, dealing with conventional mail and packages, and providing up-to-date information on the firm's website about how to reach firm personnel working remotely. The failure to take such steps is inconsistent with a lawyer's and his or her firm's obligations under Rule 1.1.<sup>49</sup> It is highly unlikely these contingency plans envisioned that lawyers and staff could infect one another with a deadly virus if they were working in close proximity. Similarly, before the pandemic, it could not be expected that law firms would not have adequate PPE supplies. Still, there is nothing to prohibit law firms from meeting with their clients provided the requirements of Rules 1.4(a)(2) and (5) are followed.<sup>50</sup>

In many cases, COVID-19 produced situations where many clients urgently need to obtain the advice of counsel. Under the Rules, clients must have the ability to initiate communications with their lawyers. Lawyers must ensure that their clients have instructions about how they can be contacted.

Even during a crisis, pursuant to Rule 1.4(b), lawyers have the duty to "explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."<sup>51</sup> Comment 1 to Rule 1.4 states: "Reasonable communication between the lawyer and the client is necessary for the client effectively to participate in the representation."<sup>52</sup> Clients cannot participate in representations if they cannot contact their lawyers. A lawyer's obligations under Rule 1.4 include to:

---

49. See James M. McCauley, *Meeting Your Ethical Responsibilities During the COVID-19 Global Pandemic*, VA. STATE BAR 2 (Apr. 9, 2020), [https://www.vsb.org/docs/Ethics\\_COVID.pdf](https://www.vsb.org/docs/Ethics_COVID.pdf) [<https://perma.cc/WN6D-D5Q7>] (indicating Rule 1.1 remains in force even during a pandemic).

50. Model Rule 1.4(a)(2) and (5) indicates:

A lawyer shall . . . (2) reasonably consult with the client about the means by which the client's objectives are to be accomplished; . . . and (5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

MODEL RULES OF PROF'L CONDUCT R. 1.4.

51. *Id.*

52. *Id.* at R. 1.4 cmt. 1.

- Ensure that clients have the lawyers' best contact information (e.g., mail, e-mail, telephone, text) and clear instructions on how communications will be handled;
- Inform clients of all upcoming court appearances, deadlines, or any other matter that requires the client's attention or participation;
- Inform clients of the law firm's "succession plan" in case a lawyer becomes ill or is otherwise unable to handle a client matter;
- Ask the client whether his or her health condition or health concerns make it unlikely for the client to appear in court, meet in person, sign documents, attend closings, or participate in pretrial activities; and
- Reduce potential problems with respect to communications with well-crafted retainer agreements, which might be supplemented by outlining the procedures that the law firm will follow in the COVID-19 pandemic. Such agreements cannot lessen the lawyers' obligations to their clients, merely clarify.<sup>53</sup>

Since clients are potential COVID-19 vectors, it is understandable that lawyers will be apprehensive about in-person contact with them until they are both vaccinated. As clients and their representatives may be infected with the COVID-19 virus and, consequently, not sufficiently healthy to deal with certain legal matters, attorneys should ascertain who might act on their behalf.

Remote communication tools often demand the use of certain security protocols. Security protocols must be acquired and deployed to ensure that all confidential or private communications with colleagues, clients, judicial officials, etc., are secure, encrypted, and only authorized persons have decryption tools.

While videoconferencing has existed for many years, relatively little thought has been given to the risks it creates.<sup>54</sup> Some lawyers have stressed

---

53. See *Ethics in the COVID-19 Pandemic*, STATE BAR OF MICH., <https://www.michbar.org/opinions/ethics/COVID-19> [https://perma.cc/XVY8-P8FM] (discussing how lawyers may meet their ethical obligations during COVID-19 and other pandemics).

54. See Nico Grant, *Zoom Says It's Being Probed by SEC, Two U.S. Attorneys Offices*, BLOOMBERG (Dec. 18, 2020, 6:41 PM), <https://www.bloomberg.com/news/articles/2020-12-19/zoom-says-it-is-being-probed-by-sec-two-u-s-attorneys-offices> [https://perma.cc/UPE4-NJYW] (noting Zoom Video Communications "provided information to multiple U.S. prosecutors and regulators regarding interactions with China and other overseas governments, as well as security and user privacy matters");

the importance of knowing who might be in the virtual rooms during a video conference. For example, a video conference might provide an opportunity to coach witnesses with written notes outside the view of the camera.<sup>55</sup>

Rule 1.4 means that lawyers are obligated to address a wide range of issues resulting from COVID-19. If law firms had some concern about the timeliness and quality of their work, they should share this concern with their clients. Law firms are obligated to arrange for their clients' possible attendance at court hearings, settlement conferences, etc.<sup>56</sup>

The duty to communicate during the COVID-19 crisis also encompasses the lawyer's responsibility to explain to clients how current events may affect their case and provide details as to the ways in which the lawyer is responding to these events. Clients need to be advised of any changes to office hours, court closings, and scheduled court appearances. Even if there is nothing pressing in a client's case, lawyers should consider sending a brief message to reassure clients that, despite this crisis, their matters are important and are not being neglected.

Similarly, communicating with opposing counsel and third parties is crucial not just for the lawyer's representation of a client but also for purposes of professionalism. Communicating expectations or delays during these difficult times helps ensure all involved are on the same page and potentially prevents frustration or future disputes over deadlines.

### B. Confidentiality

If law firms have written practices outlining policies to protect confidential information, it behooves them to re-examine them considering the COVID-19 pandemic, particularly because Rule 1.6 (Confidentiality of Information) cannot be considered separately from Rules 1.1 (Competence) and Rule 1.4 (Communications).

---

*see also* Kari Paul, *Worried About Zoom's Privacy Problems? A Guide to Your Video-Conferencing Options*, GUARDIAN (Apr. 09, 2020, 1:00 AM), <https://www.theguardian.com/technology/2020/apr/08/zoom-privacy-video-chat-alternatives> [<https://perma.cc/2MWE-QM8Y>] (referring to cybersecurity issues involving online video conferencing platforms); Rae Hodge, *Zoom Security Issues: Zoom Buys Security Company, Aims for End-to-End Encryption*, C|NET (May 08, 2020, 12:23 PM), <https://www.cnet.com/news/zoom-security-issues-zoom-buys-security-company-aims-for-end-to-end-encryption/> [<https://perma.cc/VT9G-W92H>] (detailing negative events such as Zoombombings).

55. See Rosen, *supra* note 3 (noting the need to ensure that an attorney is not giving help to a witness during a virtual court event where it would not be otherwise permitted).

56. See Neil J. Wertlieb et al., *Legal Ethics and the Coronavirus*, CAL. LAWS. ASS'N, <https://calawyers.org/california-lawyers-association/legal-ethics-and-the-coronavirus/> [<https://perma.cc/V8D4-RK25>] (suggesting methods to keep in contact and on task during COVID-19).

With certain exceptions, Rule 1.6 requires lawyers to “make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”<sup>57</sup> The universe of confidential information relating to the representation of clients is broad; consequently, “lawyers working remotely or from other irregular or nontraditional sites must carefully consider the security and confidentiality of their policies, procedures, and systems.”<sup>58</sup> Such information includes confidences, data, intellectual property, personal and private information, and secrets. In addition, it includes other information acquired or developed during representation, such as attorney work-product and law firm operational records (time sheets, telephone logs, information generated by their computers, and by other information technology systems).

Law firms should already have policies in place related to the confidentiality of information with respect to the representation of clients. It may be that such policies were prepared without adequate attention to situations where law firm attorneys and staff were working remotely. It should be kept in mind that lawyers are required to prevent employees, associates, and other law firm staff and contractors from disclosing or using confidential information. In individual cases, this may be more difficult to accomplish when people are working remotely or are inattentive due to stress-related or job-related anxiety.

When conducting a fact-based analysis to determine what is “reasonable,” certain non-exclusive factors should be considered:

- 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

---

57. MODEL RULES OF PROF'L CONDUCT R. 1.6(c).

58. Saul Jay Singer, *Legal Ethics in the Age of the Coronavirus*, DC BAR (Mar. 20, 2020), <https://www.dcbar.org/news-events/news/legal-ethics-in-the-age-of-the-coronavirus> [https://perma.cc/Y2Q5-94TZ].

- 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).<sup>59</sup>

Indeed, what is reasonable during the COVID-19 pandemic demands an inquiry to consider the advisability of different means to protect client confidentiality. This obligation may require attorneys to:

- Ensure all digital devices used for client matters are password protected so that third parties will not have access to confidential information[.]
- Set aside a private area of the home for client matters and take steps to ensure that others present cannot listen to conversations held there[.]
- Avoid using public Wi-Fi networks, deploy a VPN (virtual private network) at home, and use strong passwords and multifactor authentication to protect confidential client communications and data[; and]
- Unplugging Alexa, Google Assistant, SIRI, and other PDSs (in an abundance of caution).[<sup>60</sup>]

---

59. ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R, at 4 (2017). Comment 18 to Model Rule 1.6 states:

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 does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 18.

*See* MODEL RULES OF PROF'L CONDUCT Preamble & Scope (indicating the Rules contain a self-serving disclaimer at the beginning to the effect that their violation does not "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 . . . [as the Rules were] not designed to be a basis for civil liability"). *See generally* Gary A. Munneke & Anthony E. Davis, *The Standard of Care in Legal Malpractice: Do the Model Rules of Professional Conduct Define It*, 22 J. LEGAL PRO. 33, 41–44 (1998) (exploring the question of the definition of standard of care in the Model Rules); Ann Peters, *The Model Rules as a Guide for Legal Malpractice*, 6 GEO. J. LEGAL ETHICS 609, 611–16 (1993) (showing the use of the Model Rules and sanctions).

60. *See COVID-19 Fatigue? Don't Let Your Ethics Guard Down*, ESQUIRE DEPOSITION SOLS. (July 28, 2020), <https://www.esquiresolutions.com/COVID-19-fatigue-legal-ethics> [<https://perma.cc/YGE3-5J2V>] (providing examples of areas where client data or security could be compromised as a result of working in an online environment); Crystal Tse & Jonathan Browning, *Locked-Down Lawyers Warned Alexa Is Hearing Confidential Calls*, BLOOMBERG (Mar. 20, 2020, 11:59 AM), <https://>

Lawyers, paralegals, and other law firm personnel should follow their law firms' WFH policies. For example, how should the exchange of written documents and other materials be accomplished? How should large-scale discovery projects be organized and supervised?

When working with documents containing confidential information, the lawyers should mark as "privileged and confidential" those portions of the documents (or entire documents) that are sensitive to prevent their inadvertent disclosure. Another approach might be to append a message or "disclaimer" to client emails.

Rule 4.4(b) obligates a lawyer who "knows or reasonably should know" that he 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.<sup>61</sup> A clear, conspicuous, and appropriately used disclaimer may affect whether a recipient lawyer's duty under Rule 4.4(b) for inadvertently transmitted communications is satisfied.

### C. Competence

Lawyer professional competence can be divided into two categories. The first category includes mastery of an area of the law as well as competence in the use of technology. Rule 1.1 requires lawyers to have "the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."<sup>62</sup>

Before taking on a particular matter, lawyers should have knowledge of a particular subject, such as company law, contract law, criminal law, family law, or labor law. If they do not, they should at least be under the supervision of a lawyer who does. It is advisable that lawyers be familiar with the outlines of government programs that could both have an impact on their client's operations—such as in the areas of banking, labor, or real estate—as well as provide a source of funds for continued operations.<sup>63</sup>

---

[www.bloomberg.com/news/articles/2020-03-20/locked-down-lawyers-warned-alexai-s-hearing-confidential-calls](http://www.bloomberg.com/news/articles/2020-03-20/locked-down-lawyers-warned-alexai-s-hearing-confidential-calls) [<https://perma.cc/R8BK-3TLN>] (highlighting the dangers of products like Alexa and Siri); *Police Request Alexa Recordings to Help Solve Murder*, SENSEI ENTERS., INC. (Nov. 7, 2019), <https://senseient.com/?s=alexai> [<https://perma.cc/5SRA-2JKH>] (discussing a story of police using data saved by an Amazon Alexa to solve a murder).

61. MODEL RULES OF PROF'L CONDUCT R. 4.4(b).

62. MODEL RULE OF PROF'L CONDUCT R. 1.1.

63. See *Coronavirus (COVID-19): Small Business Guidance & Loan Resources*, U.S. SMALL BUS. ADMIN., <https://www.sba.gov/page/coronavirus-covid-19-small-business-guidance-loan-resources> [<https://perma.cc/7HCY-ZHPK>] (listing small business resources to help recover from COVID-19); *Coronavirus Relief Options*, U.S. SMALL BUS. ADMIN., <https://www.sba.gov/funding-programs/>

Except in cases of emergency, lawyers should not begin new tasks in this area unless the client specifically requests assistance.

Rule 1.1's Comment 8 requires that lawyers "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."<sup>64</sup> With respect to technology, lawyers without experience working remotely would need to arrange that people were available to assist them in acquiring the necessary skills or that other people would complete the tasks in question.

The second type of competence concerns being competent in following administrative or legal procedures—it has a dynamic aspect, that is the ability to operate in changing circumstances. Lawyers must know (or be capable of ascertaining) the relevant procedures and successfully follow them. As a result of the pandemic, judicial and governmental bodies often modify their regulations and rules, such as changing deadlines for submitting particular documents, notarization, and signatures.<sup>65</sup>

As a result of COVID-19, clients are more likely to seek advice from lawyers on topics outside their areas of specialization. Rule 1.1's Comment 3 provides that:

In an emergency a lawyer may give advice or assistance in a matter in which the lawyer does not have the skill ordinarily required where referral to or consultation or association with another lawyer would be impractical. Even in an emergency, however, assistance should be limited to that reasonably necessary in the circumstances, for ill-considered action under emergency conditions can jeopardize the client's interest.<sup>66</sup>

To the extent feasible, lawyers should only undertake such emergency measures with their clients' informed consent (preferably memorialized in

---

loans/coronavirus-relief-options [<https://perma.cc/8E2H-L394>] (linking to government support resources for COVID-19 relief); *Coronavirus Tax Relief and Economic Impact Payments*, IRS, <https://www.irs.gov/coronavirus-tax-relief-and-economic-impact-payments> [<https://perma.cc/G4SG-TJ8J>] (compiling resources to help tax filers during COVID-19); Brianna McGurran & Kelly Anne Smith, *List of Coronavirus (COVID-19) Small Business Loan and Grant Programs*, FORBES (Apr. 10, 2020, 9:17 AM), <https://www.forbes.com/sites/advisor/2020/04/10/list-of-coronavirus-covid-19-small-business-loan-and-grant-programs/?sh=72ec2edccc4b> [<https://perma.cc/5VS2-D6Z9>] (gathering state and federal resources for businesses in need of help after COVID-19).

64. MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 8.

65. See *COVID-19 Fatigue? Don't Let Your Ethics Guard Down*, *supra* note 60 (indicating an attorney has an ethical obligation to "[s]tay current with revised procedures in all relevant courts and government offices").

66. MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 3.

some fashion); the failure to do so can risk exposure to potential legal malpractice claims.<sup>67</sup>

This language presents a vital question: what constitutes an “emergency”? This issue can only be determined by examining the relevant circumstances of a situation. The characteristics of an emergency in the health and safety context differ from one involving financial matters.<sup>68</sup>

In addition to the above-described forms of competence, lawyers should familiarize themselves generally with various governmental programs that could benefit their clients.

#### D. *Diligence*

For the foreseeable future, COVID-19 is likely to increase law firm inefficiencies.<sup>69</sup> The extent to which this occurs can be limited if lawyers are diligent in their efforts and seek to act in accordance with the Rules. Rule 1.3 states that a lawyer “shall act with reasonable diligence and

---

67. *Id.*

68. See Anjelica Cappellino, *Injunctive Relief in the Age of COVID-19*, EXPERT INST. (Aug. 31, 2020), <https://www.expertinstitute.com/resources/insights/injunctive-relief-in-the-age-of-COVID-19/> [https://perma.cc/2HT6-FATF] (“Courts across the country have been implementing new procedures to accommodate the pandemic—sometimes resulting in the limited ability to file a new lawsuit.”).

The ABA Special Committee on Disaster Response and Preparedness’s Guide to Disaster Planning encourages law firms to develop business continuity plans to:

1. Create internal and external messaging regarding the firm’s status and ability to operate;
2. Coordinate with records management to ensure that incoming documents are being stored securely and that records are accessible as necessary;
3. Ensure that attorneys are performing analyses to identify and prioritize urgent matters, including docketing litigation deadlines and court appearances; and
4. Identify firm leadership responsible for responding to questions about essential firm functions.

Gericke & Winokur, *supra* note 14 (citation omitted).

69. See Adam Gorlick, *The Productivity Pitfalls of Working from Home in the Age of COVID-19*, STANFORD | NEWS (Mar. 30, 2020), <https://news.stanford.edu/2020/03/30/productivity-pitfalls-working-home-age-COVID-19/> [https://perma.cc/MME4-ZA87] (providing examples of factors impacting efficiency while working from home). See generally Benjamin Laker, *Working from Home Is Disliked by and Bad for Most Employees, Say Researchers*, FORBES (Aug. 24, 2020), <https://www.forbes.com/sites/benjaminlaker/2020/08/24/working-from-home-is-disliked-by-and-bad-for-most-employees/?sh=2087a77c6734> [https://perma.cc/D538-ZHGH] (discussing one study concerning working from home, the results of which are inconsistent with many others).

promptness in representing a client.”<sup>70</sup> When working from home, this is not always possible.

Rule 1.3’s Comment 1 provides that lawyers “should pursue [matters] on behalf of [clients] despite opposition, obstruction or personal inconvenience to the lawyer[s], and take whatever lawful and ethical measures are required to vindicate [the clients’] cause[s] or endeavor[s].”<sup>71</sup> This broad language can be problematic. When people are working from home, the divide between work time and personal time can become blurred. Clients and law firm personnel may not respect a lawyer’s right to be “off-duty.” Comment 2, which states, in part, that a “lawyer’s work load must be controlled so that each matter can be handled competently,” does not begin to address this subject.<sup>72</sup>

Rule 1.3 must be understood in conjunction with other Rules. For example, the concept of “diligence” is present when examining issues such as “communication” and “competence.”<sup>73</sup> Again, the word “reasonable” is important here. As a result of the COVID-19 pandemic, lawyers must consider the scope and scale of legal services they can provide clients due to limited technical capabilities (such as the inability to work remotely) and staffing without assistance from others. Expectations in this area depend to a great degree on the relevant practice area.

In doing their work, lawyers need to consider their own and their colleagues’ health. If lawyers become seriously ill or incapacitated (due to COVID-19 or otherwise), they should have in place a plan setting out who will cover for them. While in larger firms, this is likely something that can be handled internally, it can pose a major problem for solo practitioners or small firms. In either case, the affected clients should be informed immediately of the situation as it develops.

Personnel shortages may occur because of governmental, judicial, and the medical communities’ efforts to protect the public welfare and due to actual illness and family commitments. The shortage might not be easily offset, as it could be difficult to hire and train temporary workers who can be trained and integrated into the law firm’s communication and other relevant systems without jeopardizing security. Since this is a dynamic situation, law firms

---

70. MODEL RULES OF PROF'L CONDUCT R. 1.3.

71. *Id.* at R. 1.3 cmt. 1.

72. *Id.* at R. 1.3 cmt. 2.

73. See *id.* at R. 1.3 (discussing diligence); *id.* at R. 1.1 (discussing competence); *id.* at R. 1.4 (discussing communication).

need to explore ways they might be able to work remotely and effectively from a technical perspective.

While there is some evidence to suggest that lawyers and legal staff working from home in certain situations can be more productive than those working in their offices,<sup>74</sup> this topic requires significantly more study.<sup>75</sup> Personnel living with their children who are not attending school on a full-time basis or acting as caregivers to elderly parents are less productive<sup>76</sup> than while working from their offices.<sup>77</sup>

---

74. See David Dorion, *Working Remotely: How It's Impacting the Legal Industry and Your Firm*, LAW CROSSING, <https://www.lawcrossing.com/employers/article/900048761/Working-Remotely-How-It-s-Impacting-the-Legal-Industry-and-Your-Firm> [<https://perma.cc/SQ4G-MFZD>] (noting the benefits of working from home); Jay Harrington, *How to Stay Productive While Working From Home*, LAW.COM (Aug. 21, 2020, 2:15 PM), <https://www.law.com/2020/08/21/how-to-stay-productive-while-working-from-home> [<https://perma.cc/U2XH-9V6L>] (discussing innovations in the office during COVID-19); Jeffreys, *supra* note 23 (according to survey data from June 2020, 67% of lawyers and legal staff, given the option, would prefer to work from home).

75. See generally LITIFY, HOW TO MANAGE A REMOTE LAW FIRM (THE COMPLETE GUIDE), <https://litify.draft.click/manage-remote-law-firm> [<https://perma.cc/P2YP-THEU>] (examining topics such as how to work collaboratively, how to communicate with clients remotely, how to manage documents, and software to consider purchasing); *Remote Work Resource Hub*, LITIFY, <https://www.litify.com/remote-work> [<https://perma.cc/L6MR-C2BA>] (noting firms cannot expect employees to work solely from their offices).

76. See Anshu Siripurapu, *The Economic Effects of Working from Home*, COUNCIL ON FOREIGN RELS. (July 16, 2020, 8:00 AM), <https://www.cfr.org/in-brief/economic-effects-working-home> [<https://perma.cc/J8EX-X633>] (explaining while “[r]emote work [may] increase worker productivity, . . . it can lead to isolation and stress as the line between work and home blurs”); VALOIR, THE REAL PRODUCTIVITY IMPACT OF REMOTE WORK 2 (2020), <https://static1.squarespace.com/static/5db8a4995630c6238ccb4c26/t/5ecc114b250a6a0b1b056e7/1590432078145/Valoir+Report+-+The+real+productivity+impact+of+remote+work.pdf> [<https://perma.cc/7YAA-A9MT>] (suggesting that working from home has only a marginal negative effect on productivity, though it might be favored by employees); Vala Afshar, *Working from Home: Average Productivity Loss of Remote Work Is 1%*, ZDNET (May 11, 2020, 12:32 AM), <https://www.zdnet.com/article/the-average-productivity-loss-of-remote-work-is-1> [<https://perma.cc/UU37-6HE6>] (discussing a study detailing the impact of changing from an office to a work-from-home arrangement).

77. See Kate Whiting, *Most Leaders Think Remote Working Will Hit Productivity - This Is Why*, WORLD ECON. F. (Oct. 21, 2020), <https://www.weforum.org/agenda/2020/10/remote-working-productivity-future-of-jobs> [<https://perma.cc/75R4-4KWN>] (reporting COVID-19 is believed to harm business productivity); Brandon Vigliarolo, *Long-Term Remote Work Is Leading to a Global Drop in Productivity*, TECHREPUBLIC (July 28, 2020, 6:05 AM), <https://www.techrepublic.com/article/long-term-remote-work-is-leading-to-a-global-drop-in-productivity> [<https://perma.cc/LP9C-PDKS>] (displaying the impact of remote work on business-critical apps); Chris Mills Rodrigo, *Productivity, Fatigue, Cybersecurity Emerge as Top Remote Work Concerns*, HILL (Sept. 25, 2020, 6:00 AM), <https://thehill.com/policy/technology/517671-productivity-fatigue-cybersecurity-emerge-as-top-remote-work-concerns> [<https://perma.cc/GD3M-2GW2>] (noting fatigue can be a by-product of working remotely).

Some observers and academics have suggested that informal communications and in-person contacts are essential for organizations to develop a cohesive work culture, which is critical over the long term. Atomized law firms are unlikely to be successful, except in the short term. Also, it is far from clear whether most senior lawyers can remotely supervise subordinate attorneys and staff projects in an effective and efficient manner. This situation will make it more difficult for lawyers to deliver their work product to clients in a timely fashion.

As a result, to the extent appropriate, lawyers should seek extensions of applicable deadlines needed to allow for completion of work, and if possible, ascertain the willingness of opposing counsel to agree to new deadlines and remote operations (e.g., depositions, hearings, etc.). Lawyers should be cautious about using COVID-19 as an excuse to delay litigation longer than necessary. Rule 3.2 prohibits lawyers from using means that have no substantial purpose other than to delay or prolong the proceeding or to cause needless expense.<sup>78</sup>

#### E. *Supervising Subordinate Attorneys and Staff*

Rule 5.1 requires that lawyers having “managerial authority in a law firm . . . 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.”<sup>79</sup> Lawyers with managerial authority in the law firm share the aforementioned responsibilities with any lawyer having “direct supervisory authority over another lawyer” and “shall make reasonable efforts to ensure that the other lawyer conforms to” their ethical obligations.<sup>80</sup>

Rule 5.2 provides that subordinate lawyers should observe the Rules’ requirements and are found not to have violated them if directed by a supervisory lawyer, provided that such instructions were “reasonable.”<sup>81</sup>

---

78. MODEL RULES OF PROF'L CONDUCT R. 3.2 (“A lawyer shall make reasonable efforts to expedite litigation consistent with the interests of the client.”).

79. *Id.* at R. 5.1; see Ethan S. Burger, *The Use of Limited Liability Entities for the Practice of Law: Have Lawyers Been Lulled into a False Sense of Security?*, 40 TEX. J. BUS. L. 175, 188–90 (2004) (suggesting it is often possible to recharacterize instances of alleged partner vicarious liability as direct liability for failing to establish and implement adequate supervisory measures within a law firm).

80. MODEL RULES OF PROF'L CONDUCT R. 5.1.

81. *See id.* at R. 5.2 (“A subordinate lawyer does not violate the Rules of Professional Conduct if that lawyer acts in accordance with a supervisory lawyer’s reasonable resolution of an arguable question of professional duty.”).

This Rule does not establish a basis to make law firm partners vicariously liable for the actions or inactions of other lawyers within their firm.<sup>82</sup>

Rule 5.3 concerns lawyer assistance (i.e., both staff employees and contract workers).<sup>83</sup> An important subset of such individuals is persons who organize and Bates stamp documents and are responsible for physical evidence, as well as those who deal with lawyers' timesheets, purchases and bill paying, client funds, and deposits. It is worth noting that Rule 1.15 requires funds to be deposited into client trust accounts and other property to be placed into safe deposit boxes as soon as practicable—some of these tasks cannot be performed remotely.<sup>84</sup>

As a result of the pandemic, lawyers are likely to find it difficult to estimate with precision the amount of time needed to perform various law firm projects. More client work may need to be delegated to other lawyers or nonlawyer assistants (e.g., law clerks or paralegals) within their firm than is typical. Since many firms have been forced to reduce their staff, lawyers may have to seek the assistance of firm personnel with whom they have not worked previously. This can lead to imprecision when estimating the time needed to perform certain tasks.

In such instances, lawyers need to find ways to monitor the productivity of persons to whom work has been delegated.<sup>85</sup> It is especially important to develop online monitoring capabilities for a workflow where the failure to perform the relevant work on time could have billing or legal malpractice implications. The failure to monitor personnel workflow can give rise to circumstances where the costs involved to complete tasks exceed allotted budgets. If assignments are taking longer to complete than anticipated, it may prove impossible to find and recruit additional people for the effort. It

---

82. *Id.*; see Douglas R. Richmond, *Subordinate Lawyers and Insubordinate Duties*, 105 W. VA. L. REV. 449, 461–70 (2003) (noting Rule 5.2 makes lawyers responsible for their actions and does not allow them to shift blame to a superior who instructed them).

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

84. See *id.* at R. 1.15 (distinguishing between how lawyers handle their funds versus the funds of clients).

85. See Jeffrey H. Ruzal & Carley Baratt, *COVID-19, Work-from-Home Policies, and Maintaining Wage and Hour Compliance*, WAGE & HOUR DEF. BLOG (Mar. 10, 2020), <https://www.wagehourblog.com/2020/03/articles/wage-hour-class-actions/covid-19-work-from-home-policies-and-maintaining-wage-and-hour-compliance/> [https://perma.cc/J4AD-GALY] (“It is important for employers to track the type of telework performed by their exempt workforce.” (emphasis omitted)); KEN SATKUNAM, NORTHSTAR TECH. GRP., HOW TO MAKE YOUR LAW FIRM 200% MORE EFFICIENT 2 (2020), <https://legal.northstartechnologygroup.com/optin1600096464818> [https://perma.cc/8TXE-NJY9] (describing automatable processes that will improve law firm operations); see also Wertlieb et al., *supra* note 56 (discussing supervision and the delegation of duties during COVID-19).

is possible, if not likely, that law firms lacking experience with working remotely or using attorneys working outside their typical practice areas will generate time charges that cannot be passed on to their clients without risking a collection problem or jeopardizing their relationship, in part because such clients, during the pandemic, may be experiencing financial difficulties.<sup>86</sup>

#### F. COVID-19 and the Unauthorized Practice of Law

In response to the pandemic, many people chose to move from urban to less populated areas.<sup>87</sup> Lawyers are no exception. Whereas in the past it would be difficult for lawyers to continue to work on client matters from home, new technologies are allowing many of them to telecommute. Under ordinary circumstances, this might have presented a problem for lawyers who sought to work in a jurisdiction where they were not admitted pursuant to Rule 5.5(a), which addresses the unauthorized practice of law and multijurisdictional practice of law.<sup>88</sup> There is an exception, however, for lawyers providing “legal services on a temporary basis” that “arise out of or are reasonably related to the lawyer’s practice in a jurisdiction in which the lawyer is admitted to practice.”<sup>89</sup> The Comments to this Rule discuss what

---

86. See Bob Ambrogi, *87% of Law Offices Working Remotely, Survey Finds, As They Struggle to Maintain Financial Stability*, LAWSITES (Apr. 30, 2020), <https://www.lawsitesblog.com/2020/04/87-of-law-offices-working-remotely-survey-finds-as-they-struggle-to-maintain-financial-stability.html> [<https://perma.cc/N4Q7-TEHQ>] (indicating some challenges law firms faced because of COVID-19).

87. See Henry Grabar, *Will COVID Push People Out of Cities for Good?*, SLATE (July 11, 2020, 5:45 AM), <https://slate.com/technology/2020/07/covid-people-leaving-cities-exodus-suburbs.html> [<https://perma.cc/L7J5-NM22>] (discussing the effect of COVID on people from urban areas moving to less congested areas); Jeff John Roberts, *Are People Really Fleeing Cities Because of COVID? Here's What the Data Shows*, FORTUNE (July 17, 2020, 5:00 AM), <https://fortune.com/2020/07/17/people-leaving-cities-coronavirus-data-population-millennials-marriage-families-housing-real-estate-suburbs/> [<https://perma.cc/K6RR-SJLM>] (discussing the statistics of people fleeing urban areas during COVID); Heather Kelly & Rachel Lerman, *The Pandemic Is Making People Reconsider City Living. Trading Traffic for Chickens*, WASH. POST (June 1, 2020, 4:41 PM), <https://www.washingtonpost.com/technology/2020/06/01/city-relocate-pandemic/> [<https://perma.cc/N4EB-CQYH>] (showing the impact COVID had on people wanting to move from urban areas); C.J. Hughes, *Coronavirus Escape: to the Suburbs*, N.Y. TIMES (May 8, 2020), <https://www.nytimes.com/2020/05/08/realestate/coronavirus-escape-city-to-suburbs.html> [<https://perma.cc/9FSV-ZHPF>] (examining why people are leaving cities during COVID).

88. MODEL RULES OF PROF'L CONDUCT R. 5.5(a).

89. *Id.* at R. 5.5(c)(3).

could qualify as a “temporary basis” but do not offer an overarching explanation.<sup>90</sup>

In its Formal Opinion 495, the ABA Standing Committee on Ethics and Professional Responsibility weighs into the rationale for Rule 5.5:

The purpose of Model Rule 5.5 is to protect the public from unlicensed and unqualified practitioners of law. That purpose is not served by prohibiting a lawyer from practicing the law of a jurisdiction in which the lawyer is licensed, for clients with matters in that jurisdiction, if the lawyer is for all intents and purposes invisible *as a lawyer* to a local jurisdiction where the lawyer is physically located, but not licensed. The Committee’s opinion is that, in the absence of a local jurisdiction’s finding that the activity constitutes the unauthorized practice of law, a lawyer may practice the law authorized by the lawyer’s licensing jurisdiction for clients of that jurisdiction, while physically located in a jurisdiction where the lawyer is not licensed if the lawyer does not hold out the lawyer’s presence or availability to perform legal services in the local jurisdiction or actually provide legal services for matters subject to the local jurisdiction, unless otherwise authorized.<sup>91</sup>

Some ethics lawyers hope that this Formal Opinion will be followed by an appropriate change to the Rules. As noted by Anthony Davis of Clyde & Co., “ABA opinions ‘are merely advisory unless and until states actually issue their own opinions adopting the same position—or, even better, change their rules of professional conduct—in order to turn the advice into practice.’”<sup>92</sup> Indeed, COVID-19 might serve as a catalyst to amend the

---

90. *See id.* at R. 5.5 cmts. 5–6 (examining the meaning of “temporary basis”). In an abundance of caution, Richard J. Rosensweig warned:

In our virtual age it is possible for most lawyers to work from anywhere, making it tempting to represent clients wherever they may be found. Due to COVID-19, the desire to work in a safe place that happens to be on the wrong side of a border may further entice lawyers to ignore that border. However, what Rule 5.5 permits and forbids is uncertain in many such situations and can vary from jurisdiction to jurisdiction.

Richard J. Rosensweig, *Unauthorized Practice of Law: Rule 5.5 in the Age of COVID-19 and Beyond*, ABA (Aug. 12, 2020), <https://www.americanbar.org/groups/litigation/committees/ethics-professionalism/articles/2020/unauthorized-practice-of-law-rule-55-in-the-age-of-covid-19-and-beyond> [https://perma.cc/9LDN-5EYJ].

91. ABA Comm. on Ethics & Pro. Resp., Formal Op. 495, at 3–4 (Dec. 16, 2020).

92. Lyle Moran, *Ethics Attorneys Hopeful COVID-19 Will Prompt Changes in Remote Working Rules*, ABAJOURNAL (Dec. 28, 2020), <https://www.abajournal.com/web/article/ethics-attorneys-hopeful-covid-19-will-prompt-changes-in-remote-working-rules> [https://perma.cc/K9ZY-7HBF].

Rules to better correspond with the modern reality of many lawyers' cross-border practices.

#### G. *Rethinking Two Formal Opinions in the Pandemic*

Formal Opinion 477R examines what lawyers must do to secure protected client information when using electronic communications.<sup>93</sup> Here, the analysis involves an examination of the nature of the information and competence in the use of technology to defend against third party access to the data or IT system. In light of the pandemic, lawyers should reasonably account for the additional vulnerability they may have as a result of their remote operations.

Opinion 477R adopts the ABA Cybersecurity Handbook's language about "reasonable" cybersecurity standards, rejecting:

[S]pecific security measures (such as firewalls, passwords, and the like) and instead adopt[sing] a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.<sup>94</sup>

Recognizing "reasonable efforts" depends on the circumstances of a matter; the non-exhaustive list of factors that may be considered include:

- 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).<sup>95</sup>

Opinion 477R identifies seven factors that should be considered when seeking to determine the proper level of cybersecurity:

---

93. ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R, at 1 (May 22, 2017).

94. *Id.* at 4.

95. MODEL RULES OF PROF'L CONDUCT R. 1 (AM. BAR. ASS'N 2020).

- (i) the nature of the threat;
- (ii) how client confidential info[rmation] is stored and sent;
- (iii) the use of reasonable electronic security measures;
- (iv) how electronic communications should be protected;
- (v) the need to label client information as privileged and confidential;
- (vi) the need to train lawyers and nonlawyer assistants; and
- (vii) the need to conduct due diligence on vendors who provide technology services.<sup>96</sup>

The penultimate paragraph of Opinion 477R states:

Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Rule 1.6(c) requires a lawyer to make “reasonable efforts” to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.<sup>97</sup>

The opinion’s concluding paragraph makes clear that the standard for securing client information—making “reasonable efforts” to prevent . . . inadvertent or unauthorized . . . access”—operates as a floor.<sup>98</sup> In the future, higher levels of security may be established by law or as a result of agreements with clients.

Opinion 483—*Lawyers’ Obligations After an Electronic Data Breach or Cyberattack*—concerns lawyers’ responsibilities after data breaches or cyber-attacks.<sup>99</sup> For the purposes of the opinion, a “data breach” is “a data event where material client confidential 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.”<sup>100</sup> Opinion 483 recognizes that:

---

96. John G. Loughnane, *2019 Cybersecurity*, ABA (Oct. 16, 2019), [https://www.americanbar.org/groups/law\\_practice/publications/techreport/abatechreport2019/cybersecurity2019/](https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/cybersecurity2019/) [https://perma.cc/CB65-9C5E].

97. ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R, at 11 (2017).

98. *Id.*

99. ABA Comm. on Ethics & Pro. Resp., Formal Op. 483, at 1 (Oct. 17, 2018).

100. *Id.* at 4.

Many cyber events occur daily in lawyers' offices, but they are not a data breach because they do not result in actual compromise of material client confidential information. Other episodes rise to the level of a data breach, either through exfiltration/theft of client confidential information or through ransomware, where no client information is actually accessed or lost, but where the information is blocked and rendered inaccessible until a ransom is paid. Still other compromises involve an attack on a lawyer's systems, destroying the lawyer's infrastructure on which confidential information resides and incapacitating the attorney's ability to use that infrastructure to perform legal services.<sup>101</sup>

Opinion 483 states "Rule 1.6 is not violated even if data is lost or accessed if the lawyer has made reasonable efforts to prevent the loss or access."<sup>102</sup> This makes clear that lawyers' cybersecurity efforts should be judged by a negligence rather than a strict liability standard. Law firms must adopt reasonable measures to reduce their vulnerabilities arising from their remote operations.

Although it does not state so explicitly, Opinion 483 indicates the preparation of an incident response plan is mandatory to avoid violating Rule 1.6, but the precise contours of such a plan are not set out. Also relevant here is the potential tension between the client's right to confidentiality and any legal or regulatory requirements to report data breaches.<sup>103</sup>

Pursuant to Rule 1.4, lawyers are obligated to inform their current clients of data breaches that impact their material confidential information.<sup>104</sup> Knowing precisely what constitutes "material information" may be problematic because what lawyers know about a particular data breach may be imperfect or change over time. Furthermore, lawyers may not know what "material" is for their clients since the lawyers may not know the full scope of their clients' current or planned future activities. Significantly,

---

101. *Id.*

102. *Id.* at 9.

103. See David Bayne, *ABA Formal Opinion 483: What Are a Lawyer's Obligations After a Data Breach or Cyberattack?*, N.Y. L.J. (Apr. 22, 2019, 2:30 PM), <https://www.law.com/newyorklawjournal/2019/04/22/aba-formal-opinion-483-what-are-a-lawyers-obligations-after-a-data-breach-or-cyberattack/?slreturn=20210123162432> [<https://perma.cc/2H8F-259V>] ("The legal and regulatory reporting obligations are numerous, complex and are ignored at the firm's peril, but ABA Formal Ethics Opinion No. 483 reminds lawyers that there are also independent ethical obligations triggered when a cyber-attack compromises confidential client information or incapacitates a law firm's computers or network.").

104. *Id.*

Formal Opinion 483 confirms that Rule 1.9 does not establish a duty for lawyers to notify their former clients in the absence of another legal basis compelling notice.<sup>105</sup>

In October 2019, Jason Tashea reported in the *ABA Journal* that its Legal Technology Resource Center's *Legal Technology Survey Report 2019* concluded that “[l]awyers are failing at cybersecurity.”<sup>106</sup> Despite multi-million-dollar losses as a result of cyber-attacks, it seemed that at many law firms “[t]here were significant drops in the use of very standard cybersecurity practices.”<sup>107</sup> The legal community’s relatively low level of cybersecurity might have the characteristics of being a “dirty little secret” were it not already widely known.

There is a significant difference of opinion about the state of law firm cybersecurity. Some analysts seem to be pulling their punches. For example, according to one author writing in the *ABA Journal*: “Overall, the state of adoption, comfort, and facility with technology tools in the legal industry is good,” but there are some “areas where improvement can still be made.”<sup>108</sup>

### 1. Cyber Incident Awareness

It should come as no surprise that many law firms are under constant cyber-attack.<sup>109</sup> According to Karin Conroy, roughly “80% of the largest

---

105. *Id.*

106. Jason Tashea, *Lawyers Are Failing at Cybersecurity, Says ABA TechReport 2019*, ABAJOURNAL (Oct. 24, 2019, 1:36 PM), <https://www.abajournal.com/news/article/lawyers-are-failing-at-cybersecurity-says-aba-techreport-2019> [https://perma.cc/U4JZ-M8SV].

107. Dennis Kennedy, *2019 Cloud Computing*, ABA (Oct. 2, 2019), [https://www.americanbar.org/groups/law\\_practice/publications/techreport/abatechreport2019/cloudcomputing2019/](https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/cloudcomputing2019/) [https://perma.cc/2MRG-JTCK] (“The “2019 Survey highlights a major concern that, while lawyers talk the talk about security concerns . . . to a shocking degree they do not walk the walk.”).

108. Mark Rosch, *2019 Technology Training*, ABA (Nov. 27, 2019), [https://www.americanbar.org/groups/law\\_practice/publications/techreport/abatechreport2019/techtraining19/](https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/techtraining19/) [https://perma.cc/SVA5-28WY]. See Paul Rosenzweig, ‘Other Than That Mrs. Lincoln . . .’, LAWFARE (Jan. 1, 2018, 10:00 AM), <https://www.lawfareblog.com/other-mrs-lincoln-%E2%80%A6> [https://perma.cc/D3B2-2FFF] (attempting to assess the Trump administration’s efforts in cybersecurity reminding the author of the famous quip “[o]ther than that Mrs. Lincoln, how was the play?”).

109. “Cyber-attack” (alternatively “cyberattack” or “cyber attack”) does not have a universally-accepted definition. A cyber-attack can take many forms and objectives. In this Article, the term cyber-attack means “[a]n attack, via cyberspace, targeting an [organization’s] use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.” *Cyber Attack*, NIST, [https://csrc.nist.gov/glossary/term/Cyber\\_Attack](https://csrc.nist.gov/glossary/term/Cyber_Attack) [https://perma.cc/MBA8-RZCB]. The National Institute of Standards and Technology (NIST) is an agency within the U.S.

100 law firms have experienced” some variety of cybersecurity “violation.”<sup>110</sup> This situation is unlikely to change in the foreseeable future.<sup>111</sup>

The 2020 *Legal Technology Survey Report* indicated 29% of respondents had experienced security breaches such as a lost or stolen computer or smartphone, an attack from a hacker, a break-in, or a website exploit.<sup>112</sup> While this represented a 3% increase over the previous year,<sup>113</sup> given all the variables, this difference is not significant. What is notable is the 2020 Survey reported that the share of respondents who do not acknowledge

---

Department of Commerce. To get a sense of notable cyber-attacks, see the Center for Strategic and International Studies’ (CSIS) summary of “significant cyber incidents.” CSIS’s data includes “cyber-attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars.” CTR. FOR STRATEGIC & INT'L STUD., SIGNIFICANT CYBER INCIDENTS SINCE 2006 1, [https://csis-website-prod.s3.amazonaws.com/s3fs-public/201002\\_Significant\\_Cyber\\_Events\\_List.pdf](https://csis-website-prod.s3.amazonaws.com/s3fs-public/201002_Significant_Cyber_Events_List.pdf) [https://perma.cc/GAG9-6X3Q].

110. Bryan Lieber, *Law Firm Guide to Cybersecurity*, ABA (Oct. 1, 2020), [https://www.americanbar.org/groups/law\\_practice/publications/techreport/2020/lawpay-cybersecurity/](https://www.americanbar.org/groups/law_practice/publications/techreport/2020/lawpay-cybersecurity/) [https://perma.cc/K786-7CXJ] (citing Karin Conroy’s work on improving law firm cybersecurity).

111. See Neil Rose, *Law Firms Under Constant Cyber-Attack*, LEGALFUTURES (May 28, 2020), <https://www.legalfutures.co.uk/latest-news/law-firms-under-constant-cyber-attack> [https://perma.cc/9Q94-C8JR] (exploring the level and intensity of threats and cyber-attacks law firms face); Shawn Mike, *How to Prevent Cybersecurity Risks at Law Firms in 2019*, LEGALREADER.COM (June 14, 2019), <https://www.legalreader.com/prevent-cybersecurity-risks-law-firms-2019/> [https://perma.cc/R2TJ-9TRD] (“[A]ttacks, while fewer at first, are only going to increase in the future.”); Scott Putnam, *Cybersecurity for Law Firms*, DIGIT. UMBRELLA (Jan. 29, 2020), <https://www.digitalumbrella.com/2020/01/cybersecurity-for-law-firms/> [https://perma.cc/MU4S-EB7N] (“[During] the first nine months of 2019, there were 5,183 reported data breaches resulting in 7.9 billion exposed records. That [was] an increase of 33.3% in breaches and 112% in total records over the same period in 2018.”); Christine Simmons et al., *More Than 100 Law Firms Have Reported Data Breaches. And the Problem Is Getting Worse*, LAW.COM (Oct. 15, 2019, 1:10 PM), <https://www.law.com/legaltechnews/2019/10/15/more-than-100-law-firms-have-reported-data-breaches-and-the-picture-is-getting-worse/> [https://perma.cc/6SNX-ZCEG] (illustrating the extent of law firm cyber safety issues); 3 *Cyber Threats That Can Shut Down Your Law Firm*, FIELD EFFECT (July 4, 2020), <https://fieldeffect.com/covalence-law/cyber-threats-that-can-shut-down-your-law-firm/> [https://perma.cc/9EZZ-5DCM] (“Each day, the odds of a cyber attack on your law firm increase. From solo firms to the top 100, no one is immune from a targeted attack.”); Daisy McElherron, *The Threats Posed by Cyber Attacks in the Legal Industry*, SALT SECURE COMM'NS (Oct. 16, 2019), <https://saltdna.com/news/the-threats-posed-by-cyber-attacks-in-the-legal-industry> [https://perma.cc/9UCJ-R9U7] (showing the threats that cyber-attacks have on the legal field).

112. John G. Loughnane, *2020 Cybersecurity*, ABA (Oct. 19, 2020), [https://www.americanbar.org/groups/law\\_practice/publications/techreport/2020/cybersecurity/](https://www.americanbar.org/groups/law_practice/publications/techreport/2020/cybersecurity/) [https://perma.cc/R8SL-RJ9J].

113. *Id.*

knowing whether their firm has ever experienced a security breach remained relatively constant when compared to the year prior—roughly 20%.<sup>114</sup>

Although it might be counterintuitive, small firms are more likely to know that they have been breached than large firms. While the latter are more likely to have dedicated in-house cybersecurity or IT personnel engaged in monitoring the law firms' defensive systems, smaller firms are probably more aware of system-wide problems that arise.

To gauge the effectiveness of network cybersecurity systems, simulations should be used to determine their “dwell times.”

Dwell time is actually the sum of two important metrics: MTTD and MTTR. These are explained below.

- **Mean Time to Detect (MTTD):** The time it takes, on average, to detect a security incident from the time the network was compromised to the time it was detected.
- **Mean Time to Respond/Remediate (MTTR):** The time it takes, on average, to respond to or remediate a breach from the time it was detected.<sup>115</sup>

Of course, these calculations are only possible if both the time of breach and detection are known. This is probably beyond the capabilities of most law firms, which can only notify their clients of breaches after they are confirmed, at which time, under the best of circumstances, the data

---

114. *Id.*

115. Lolita Chandra, *Measuring the Effectiveness of AI in the SOC*, SEC. INTEL. (May 22, 2020), <https://securityintelligence.com/posts/measuring-the-effectiveness-of-ai-in-the-soc/> [https://perma.cc/V9QD-XSHV]. Cybersecurity specialists are not necessarily consistent in their use of the term “dwell-time.” See *Dwell Time: The Key Security Metric Every Company Fears*, ARMOR (Apr. 2020), [https://cdn.armor.com/app/uploads/2020/08/Infographic\\_DwellTime.pdf](https://cdn.armor.com/app/uploads/2020/08/Infographic_DwellTime.pdf) [https://perma.cc/N5VK-4RV6] (defining dwell time as “[t]he number of days a threat actor remains undetected within a given environment until remediation”); Asha Barbaschow, *Median ‘Dwell’ Time for Cyber Intrusion Highest in APAC at 172 Days: FireEye*, ZDNET (Jan. 11, 2018), <https://www.zdnet.com/article/median-dwell-time-for-cyber-intrusion-highest-in-apac-at-172-days-fireeye/> [https://perma.cc/XT4J-RB7M] (“The time between an attacker compromising a secured network and the breach being detected is the highest in the APAC region, with the median ‘dwell’ time 73 days above the global median of 99 days”); JOSHUA C. DOUGLAS, RAYTHEON | WEBSENSE, CYBER DWELL TIME AND LATERAL MOVEMENT THE NEW CYBERSECURITY BLUEPRINT 4, 6, [https://www.raytheon.com/sites/default/files/capabilities/rtnwcm/groups/cyber/documents/content/rtm\\_269210.pdf](https://www.raytheon.com/sites/default/files/capabilities/rtnwcm/groups/cyber/documents/content/rtm_269210.pdf) [https://perma.cc/LWZ6-74F3] (defining the term and discussing “Focus Areas To Reduce Dwell Time”: (i) “Fundamental security controls”; (ii) “Granular visibility and correlated intelligence”; (iii) “Continuous endpoint monitoring” (iv) “Actionable prediction of human behavior”; and (v) “User awareness”).

compromised can be identified. Again, the information technology and communication systems of law firms that recently transitioned to remote operations are less likely to be able to generate reliable data about the time of breach and detection.

The ABA surveys and information found in other sources are consistent in reporting that the harms law firms suffer from viruses, spyware, and malware attacks seem to be increasing. The costs of attacks typically include cybersecurity management fees to consultants for repair, downtime or loss of billable hours, expenses for replacing software or hardware, loss or destruction of files, harm to business reputation (including loss of existing clients and problems generating new clients), investigatory costs to ascertain the nature of the breach, notifying law enforcement of the breach, and remediation and revision of law firm cybersecurity policies.<sup>116</sup> The need for these expenditures is readily apparent—of course, other “adverse consequences may go unnoticed” as the actual costs of most cyber-attacks may be *de minimis* (at least initially) in terms of the number or value of records exposed.<sup>117</sup> Indeed, given imprecision in definition, variation in methodology, imperfect data collection, and the promotion of self-interest, it is common to find questionable assertions about law firm vulnerability to cyber-attacks.<sup>118</sup>

---

116. Loughnane, *supra* note 112.

117. *Id.; cf. Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES (Apr. 15, 2021), <https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> [<https://perma.cc/6Z37-WLJ6>] (providing a list of security breach laws that include provisions and requirements regarding proper compliance).

118. The cybersecurity literature is replete with unsubstantiated claims, such as “60% of small businesses that are hacked go out of business within two years.” See Robert Johnson, III, *60 Percent of Small Companies Close Within 6 Months of Being Hacked*, CYBERCRIME MAG. (Jan. 2, 2019), <https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/> [<https://perma.cc/B94Z-DFK3>] (making this claim); Joe Galvin, *60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack. Here's How to Protect Yourself*, INC. (May 7, 2018), <https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html> [<https://perma.cc/FQ4U-XL6S>] (stating the same); Luis A. Aguilar, *The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses*, U.S. SEC. & EXCH. COMM'N (Oct. 19, 2015), <https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html> [<https://perma.cc/TV9H-9FRU>] (“[A] 2012 study by the National Cyber Security Alliance, . . . found that 60 percent of small firms go out of business within six months of a data breach.”); Eric Chabrow, *60% of Hacked Small Businesses Fail. How Reliable Is That Stat?*, BANK INFO SEC. (May 3, 2017), <https://www.bankinfosecurity.com/blogs/60-hacked-small-businesses-fail-how-reliable-that-stat-p-2464> [<https://perma.cc/3MH9-YM94>] (showing even though the claim that 60% of hacked small businesses fail is misleading or false, it gets repeated frequently); Richard Bejtlich, *The Origin of the Quote “There Are Two Types of Companies”*, TAOSECURITY BLOG (Dec. 18, 2018), <https://taosecurity.blogspot.com/2018/12/the-origin-of-quote-there-are-two-types.html>.

In 2019, Dennis Kennedy reported in the *ABA Journal*:

Although lawyers say that confidentiality, security, data control and ownership, ethics, vendor reputation and longevity, and other concerns weigh heavily on their minds, the employment of precautionary security measures is quite low, with no more than 35% (down from 38%) of respondents actually taking any one of the specific standard cautionary cybersecurity measures listed in the 2019 Survey question on the topic. Seven percent of respondents reported taking NONE of the security precautions of the types listed. Only 41% of respondents report[ed] that the adoption of cloud computing resulted in changes to internal technology or security policies. These are troubling numbers.<sup>119</sup>

The 2020 Survey (based on 2019 data) indicates that, even before the COVID-19 pandemic, lawyers' compliance with even the most basic cybersecurity practices could be characterized as "lax." This data is certainly not reassuring even for the most "chill" client. After the pandemic outbreak, both the volume and scale of cyber-attacks against law firms have increased. Although COVID-19, at present, is the Biden Administration's top priority, combating cybercrime is a major concern as well.<sup>120</sup>

## 2. Incident Response Plans

The 2020 Survey response revealed that there had been a modest increase in the number of law firms developing incident response plans (34% in 2020 in contrast to 31% in 2019 and 25% in 2018).<sup>121</sup> These figures are

---

html [<https://perma.cc/48V7-3L87>] (exploring the history of the commonly used phrase, "There are two types of companies"); Robert S. Mueller, III, Director, FBI, Prepared Remarks at the RSA Cyber Security Conference: Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies (Mar. 1, 2012), <https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies> [<https://perma.cc/N7RL-Z69C>] (noting catchy phrases seem to dominate much of the discussion of complex cyber-related issues).

119. Kennedy, *supra* note 107.

120. See *The Biden-Harris Administration Immediate Priorities*, THE WHITE HOUSE, <https://www.whitehouse.gov/priorities/> [<https://perma.cc/W5V5-36M8>] (showing the Biden Administration's other top priorities are climate, racial equality, economy, health care, immigration, and restoring America's place in the world); Michael Garcia & Mieke Eoyang, *A Road Map for Tackling Cybercrime*, LAWFARE (Dec. 10, 2020, 10:34 AM), <https://www.lawfareblog.com/road-map-tackling-cybercrime> [<https://perma.cc/A75E-TNRM>] (discussing how combatting cybercrime remains a major concern).

121. Loughnane, *supra* note 112.

consistent with other private-sector entities.<sup>122</sup> Larger firms are most likely to have incident response plans, but it is impossible to assess how suitable these are for their firms' needs.

Incident response plans should be law firm-specific and consistent with all applicable laws and professional obligations. They should be informed by standards such as those set out in the National Institute of Standards and Technology (NIST) framework or equivalents, which provide an excellent basis for many points that should be included in incident response plans.<sup>123</sup>

Incident response plans envision the creation of cybersecurity policies, practices, and procedures. Even solo practitioners or small firms should develop their own plans. Typically, these plans start with how to act upon the reporting of an incident, confirmation of the incident, escalation as appropriate, and investigation.

While smaller firms can hire outside consultants to assist in the necessary work, larger firms may choose to rely on law firm personnel, adding outside assistance as necessary. Law firms are encouraged to designate an incident response project manager who can work with a cross-disciplinary team familiar with breach reporting obligations, mitigation requirements, and steps needed for recovery. Also, plans provide a post-incident review period to allow any lessons learned to be incorporated into a revised plan.<sup>124</sup> From start to finish, creating viable incident response plans and following them in the event of cyber-attacks can prove quite costly and complex—not surprisingly, they often require outside assistance.<sup>125</sup>

---

122. *Incident Response (IR)*, CROWDSTRIKE (May 6, 2021), <https://www.crowdstrike.com/cybersecurity-101/incident-response-ir-plan/> [https://perma.cc/43EX-78SK] (citing a Ponemon Survey indicating that “77% of respondents say they lack a formal incident response plan applied consistently across their organization, and nearly half say their plan is informal or nonexistent”).

123. See *Cybersecurity Framework Version 1.1*, NIST (Apr. 2018), <https://www.nist.gov/cyberframework/framework> [https://perma.cc/AUA8-QN5Z] (providing an illustrative framework for an incident response plan).

124. Cf. Loughnane, *supra* note 112 (describing other post-incident responses); *Security Breach Notification Laws*, *supra* note 117 (legislation also requires post-incident notifications of affected individuals).

125. See AT&T CYBERSECURITY, THE AT&T CYBERSECURITY INCIDENT RESPONSE TOOLKIT: PUTTING THE OODA LOOP TO WORK IN THE REAL WORLD (2020), [https://learn-cybersecurity.att.com/c/incident-response-wh?x=5v9G6V&utm\\_internal=soc-irlookbook](https://learn-cybersecurity.att.com/c/incident-response-wh?x=5v9G6V&utm_internal=soc-irlookbook) [https://perma.cc/DN8X-FGT9] (discussing how AT&T can assist client's incident detection and response needs); Carole J. Buckner, *Developing an Incident Response Plan for a Cyber Attack*, PROCOPIO (Apr. 17, 2019), <https://www.procopio.com/articles/view/cyber-attack-incident-response> [https://perma.cc/7QJX-PC4F] (describing a complete incident response process including the incident response team and incident response process).

It is vital that lawyers and their law firms re-examine and revise (or prepare) incident response plans that are consistent with their remote operations. They should conduct tabletop exercises to ascertain whether they are suitable for their needs. These efforts would be enhanced with the input of consultants as well as bar and professional organizations.

#### H. *A Need for Law Firm Ethics Counsel in the Post-Pandemic World*

In recent years, a growing number of law firms have created the position of ethics counsel (others established standing ethics committees alone or alongside an ethics counsel). Ideally, ethics counsel will be available as needed to respond to attorney or staff inquiries, review law firm policies, practices, and procedures to ensure their compatibility with relevant legal, ethical norms, and relevant decisions of the courts and state bars. In addition, ethics counsel, *sua sponte* or in response to a claim, might investigate a complaint and propose remedial actions.

COVID-19 has produced novel conditions within most law firms. A significant share of the legal literature on the role of ethics counsel relates to billing practices.<sup>126</sup> The discussion above would seem to show a wide array of matters likely to produce ethical quandaries, such as the implementation of WFH and RTW policies, problems arising from remote operations, and personnel issues connected with the performance of new tasks or the absence of trust.

Under these conditions, it might be advisable to appoint an ethics counsel, or in larger law firms, to establish an ethics committee. This individual or group might create a newsletter to discuss issues that have arisen and a resolution that might benefit others. Also, the newsletter could share other relevant information published by others. In so doing, it would decrease the chance that the improper action would occur again.

---

126. See Susan Saab Fortney, *Ethics Counsel's Role in Combating the "Ostrich" Tendency*, 2002 PRO. LAW. SYMP. ISSUES 131, 136 (2002) (showing law firm survey results on the ethics policies and systems they have implemented); Lisa G. Lerman, *Blue Chip Bilking: Regulation of Billing and Expense Fraud by Lawyers*, 12 GEO. J. LEGAL ETHICS 205, 298 (1999) (listing the possible uses for a firm's ethics counsel or committee to (i) "establish written policies on billing practices and reimbursement for expenses"; (ii) "offer regular training to partners (including managers), associates, law clerks, paralegals, secretaries, and other staff, on billing practices and other ethical issues"; and (iii) "encourage all firm employees to report possible misconduct to the ethics committee, and ensure that those employees are protected from retaliation for raising questions").

#### IV. COVID-19-RELATED LEGAL MALPRACTICE

There is no universally accepted definition for “legal malpractice.” There is agreement that it can take one or more of four “pure” forms: (i) breach of fiduciary duty, (ii) breach of contract, (iii) the tort of malpractice, and (iv) vicarious liability.<sup>127</sup> Most legal malpractice cases do not end up in the courts. Experience indicates that only a minority of potential legal malpractice plaintiffs choose to pursue their alleged claims legally. Many potential plaintiffs are deterred from making legal malpractice claims believing that they are unlikely to prevail in court or by the high cost of litigation.<sup>128</sup> Other contributing factors include the desire of plaintiffs to preserve relationships with counsel, or for public companies, the fear of triggering shareholder lawsuits.<sup>129</sup>

Often potential plaintiffs are not aware that they might have grounds for legal malpractice lawsuits. During times of recession, organizations are more likely to investigate potential claims if they suspect they may have an adequate basis to file legal malpractice lawsuits for various reasons discussed below. In a recession, clients may be inclined to bring legal malpractice cases to shift the blame for a subpar economic performance to others. Preliminary evidence suggests that this may particularly be the case for law firm clients in the aftermath of COVID-19.<sup>130</sup>

---

127. SUSAN SAAB FORTNEY & VINCENT R. JOHNSON, *LEGAL MALPRACTICE LAW: PROBLEMS AND PREVENTION* 1–30 (2008); VINCENT R. JOHNSON, *LEGAL MALPRACTICE LAW IN A NUTSHELL* 18–19 (2011). See generally ROBERT E. MALLEN & JEFFREY M. SMITH, *LEGAL MALPRACTICE* § 1.1 (5th ed. 2000) (discussing the lack of definition of legal malpractice, but recognizing it takes various forms).

128. Leslie C. Levin, *When Lawyers Screw Up*, 32 GEO. J. LEGAL ETHICS 109, 110–15 (2019) (reviewing Herbert Kritzer and Neil Vidmar’s book, *When Lawyers Screw Up: Improving Access to Justice for Legal Malpractice Victims* (2018), and examining, *inter alia*, why it is so difficult for plaintiffs to recover in legal malpractice cases). Earlier, Duke University Law School published a working paper by these authors on the same topic in a less comprehensive manner titled *When the Lawyer Screws Up: A Portrait of Legal Malpractice Claims and Their Resolution*. Herbert M. Kritzer & Neil Vidmar, *When the Lawyer Screws Up: A Portrait of Legal Malpractice Claims and Their Resolution* (Duke L. Sch., Working Paper, 2015), [https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=6182&context=faculty\\_scholarship](https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=6182&context=faculty_scholarship) [<https://perma.cc/FP3F-APDP>]; Polly A. Lord, *Loss of Chance in Legal Malpractice*, 61 WASH. L. REV. 1479, 1485–86 (1986) (advocating the application of the loss of chance doctrine to legal malpractice to reduce the harshness of the trial-within-a-trial method arising from the need to establish causation of harm suffered).

129. Geoffrey K. James & Ethan S. Burger, *Cybersecurity: The Achilles Heel of Today's Global Law Departments*, ACC DOCKET (Nov. 27, 2019), <https://m.acc.com/docket/articles/cybersecurity-achilles-heel-global-law-departments.cfm> [<https://perma.cc/DFZ4-QZS4>].

130. Andrew Lavoott Bluestone, *Legal Malpractice in the Time of Plague*, N.Y. L.J. (Sept. 8, 2020, 10:00 AM), <https://www.law.com/newyorklawjournal/2020/09/08/legal-malpractice-in-the-time-of>

Many professional liability insurance policies provide for mandatory arbitration of disputes. Disagreements between the insurance companies and their insureds are often resolved through mediation. Thus, data from insurance companies on the characteristics of the claims they receive from insureds are useful but imperfect indicators of the scope and scale of legal malpractice occurring in the United States.<sup>131</sup> Still, the insurance industry reports an increase in the number of legal malpractice claims it is seeing relating to COVID-19 and such information should be regarded as reliable for the types of law firms it insures.<sup>132</sup>

In June 2020, the ABA organized a continuing legal education program called *Looking Backward to Predict the Future: COVID-19's Anticipated Impact on Legal Malpractice Claims*.<sup>133</sup> The program's premise was that the insurance industry's experience with past law firm malpractice would have predictive

---

plague/ [https://perma.cc/DL8Z-7NW7]; Alanna Clair & Shari Klevens, *Minimizing the Risk of Legal Malpractice Claims Amid a Pandemic*, JDSUPRA (June 10, 2020), https://www.jdsupra.com/legalnews/minimizing-the-risk-of-legal-98557/ [https://perma.cc/9UF7-UHS].

131. Legal malpractice insurance coverage comes in two “pure” varieties: “Claims–Made and Reported Coverage” and “Occurrence Coverage” are the most common types of policies:

**Claims–Made and Reported Coverage:** Most professional liability policies are written on this basis. In order for a claim to be covered, the claim must be first made against the insured lawyer and reported to the insurance company during the policy period. Some policies may be “claims–made” forms, where the claim must be made during the policy period, but the insured’s requirement to report the claim to the insurance company may extend to a time period beyond the expiration of the policy period (such as “within a reasonable period of time” or “as soon as practicable”).

**Occurrence Coverage:** A policy that provides coverage for claims arising from acts or omissions occurring during the period of time covered by the policy, regardless of when the claim is actually made. This form of coverage is very familiar to most consumers, and while it is used for many casualty insurance products (such as auto and homeowners insurance), it is rarely used for professional liability coverage.

*FAQs on Extended Reporting (“Tail”) Coverage*, ABA (Apr. 18, 2013), https://www.americanbar.org/groups/lawyers\_professional\_liability/resources/extended\_reporting\_coverage/#top [https://perma.cc/42S3-MQUJ].

132. Eileen Garczynski & Melissa M. Lessell, *Looking Backward to Predict the Future: COVID-19's Anticipated Impact on Legal Malpractice Claims* [CC] (June 26, 2020), https://www.americanbar.org/events-cle/ecd/ondemand/400906375/ [https://perma.cc/4UNS-UGNE] (transcript available from the ABA); LEMME LAW FIRM PRAC. TEAM, LEMME INS. BROKERS & CONSULTANTS, STATE OF THE INSURANCE MARKET LAWYERS' PROFESSIONAL LIABILITY REPORT 4 (2020), https://epicbrokers.com/wp-content/uploads/2020/04/EPIC-LPL-Report\_Market-Conditions-March-2020.pdf [https://perma.cc/BKR5-VLHA]; Judy Greenwald, *Legal Malpractice Insurers See Increase in Claims: Report*, BUS. INS. (May 20, 2020), https://www.businessinsurance.com/article/20200520/NEWS06/912334663/Legal-malpractice-insurers-see-increase-in-claims-Report [https://perma.cc/EZ4N-P2ML].

133. Garczynski & Lessell, *supra* note 132.

value for the types of claims made due to COVID-19. Eileen R. Garczynski, Senior Vice President and Ames & Gough's Partner, an insurance broker specializing in professional liability insurance, along with Melissa M. Lessell, Partner at Deutsch Kerrigan, reported that they were witnessing a significant uptick in legal malpractice claims after the outbreak of the pandemic, similar to that which occurred after the 2008 recession. Historical data drawn from (i) the ABA and (ii) Ames & Gough surveys show that common bases for legal malpractice claims were:

- *Failure to Know/Properly Apply the Law;*
- *Planning Error[s]/Wrong Procedural Choice[s];*
- *Inadequate Discovery/Investigation;*
- *Drafting Error[s];*
- *Failure to Obtain Consent/Inform Client[s]; and*
- *Failure to Calendar Properly.*<sup>134</sup>

In contrast, Garczynski and Lessell predicted that the “Most Likely Errors During and Post-COVID-19/Economic Downturn” period will probably be:

- **Administrative errors[.]** Work from home-related issues/human element, suspension of legal deadlines, clarity of tolling provisions, reduced staff, technology issues, COVID-19 Scheduling changes, mail not attended to, etc.[.]

---

134. *Id.* at 20. The ABA Standing Committee on Lawyers' Professional Liability has been collecting and publishing legal malpractice data since 1985. The data is reported by nine commercial carriers and thirteen national associations of bar-related insurance companies. These law firms are primarily small and medium size. The ABA 2016–2019 study is now available. See Robert Anthony Gottfried & Jessica R. MacGregor, *Profile of Legal Malpractice Claims 2016–2019* (2020), <https://www.americanbar.org/products/inv/book/405555870> [<https://perma.cc/6DBM-RA8V>]. In contrast, Ames & Gough's 2020 report on legal malpractice claims covers claims reviewed or insured by “10 leading legal malpractice insurers . . . [that] provide insurance to approximately 80% of both the AM LAW 100 and NLJ 250 firms.” AMES & GOUGH, LPLI 2020 CLAIMS SURVEY: LAW FIRMS STRUGGLE WITH RISING MALPRACTICE CLAIMS 1 (2020) (on file with author) [hereinafter AMES & GOUGH, LPLI 2020 CLAIMS SURVEY]. Copies of this survey may be obtained by emailing: info@amesgough.com, with “LPLI Claims Survey 2020” in the subject line.

- **Failure to Know the Law[.]** Taking on work outside your area of expertise and/or regulations changing quickly and not staying on top of them; Res Nova Issues[;]
- **Negligence/Failure to Communicate[.]** Staying [within] the scope of engagement; documenting conversations; notifying [clients, witnesses, etc.] of pending deadlines, communicating potential costs/verdicts/outcomes [to clients;]
- **Fraud[.]** Ponzi Schemes[;]
- **Lack of Supervision[.]** Classic Lone Wolf scenarios, [Junior] Staff not being supervised, Wellness-Related Concerns[;]
- **Counter Claims vs. Suit for Fees[.]** Closely watch Account Receivables[; and]
- **Cyber Related Legal Malpractice Claims[.]** 131% increase in hacks [over the prior year].<sup>135</sup>

While these instances of legal malpractice were mostly linked to the direct consequences of working remotely, such as the use of unfamiliar technology, Garczynski and Lessell emphasized the importance of human factors such as lawyer mental health and substance abuse.<sup>136</sup> Lawyers can

---

135. Garczynski & Lessell, *supra* note 132, at 23–24 (2020). Lawyers should understand that suing clients to collect owed fees frequently triggers claims for legal malpractice; consequently, lawyers should weigh the risks before bringing such actions. MALLEN & SMITH, *supra* note 127, at § 2.15; Greg Fayard, *Avoiding Legal Malpractice Tip: Don't Sue Your Client for Fees*, FMG LAW (June 17, 2019), <https://www.fmglaw.com/FMGBlogLine/professional-liability/avoiding-legal-malpractice-tip-dont-sue-your-client-for-fees> [<https://perma.cc/7QX3-UGAH>]; *Attorney Malpractice—Suing Client to Collect Unpaid Legal Fees*, L SQUARED INS. AGENCY (Mar. 10, 2017), <https://www.l2insuranceagency.com/blog/attorney-malpracticesuing-client-to-collect-unpaid-legal-fees.aspx> [<https://perma.cc/AHM4-U3G6>]. One should recognize that all do not accept this view. One consulting firm that examined the post-pandemic legal market urged “more rigor around billing and collections” as “a primary driver of revenue growth.” CITI PRIVATE BANK & HILDEBRANDT CONSULTING LLC, 2021 CLIENT ADVISORY 11 (2020), <https://www.privatebank.citibank.com/ivc/docs/2021CitiHildebrandtClientAdvisory.pdf> [<https://perma.cc/LE72-5CBY>].

136. Garczynski & Lessell, *supra* note 132, at 23, 33; see also James Gray Robinson, *Lawyers, Addiction and COVID-19: ‘Changing the Landscape for Everyone’*, ABAJOURNAL (June 4, 2020), <https://www.abajournal.com/voice/article/attorneys-addiction-and-covid19> [<https://perma.cc/BA43-GDVV>] (describing the same factors); *Mental Well-Being Resources for Lawyers During COVID-19*, HINSHAW (Mar. 23, 2020), <https://www.hinshawlaw.com/newsroom-newsletters-335.html> [<https://perma.cc/5LK4-59B3>] (providing resources for stress reduction); Staci Zaretsky, *Lawyers and Legal Professionals Must Care for Their Mental Health Amid COVID-19 Crisis*, ABOVE THE L. (Mar. 17, 2020, 1:43 PM), <https://abovethelaw.com/2020/03/lawyers-and-legal-professionals-must-care-for-their-mental-health-amid-covid-19-crisis> [<https://perma.cc/6XEH-F46Y>] (exploring the importance of staying connected); Aebra Coe, *Virus Poses Latest Test to Supporting Atys’ Mental Health*, LAW360

reduce their stress level by avoiding practicing law outside their comfort zones (note that in most cases it is not appropriate to charge clients for such time if it is unreasonably high).<sup>137</sup> Lawyers should be sensitive to the stress that their colleagues and clients might be under.<sup>138</sup>

According to Garczynski and Lessell, post-COVID-19 areas where legal malpractice claims are most likely to arise are: (i) Real Estate, (ii) Business Transactions/Corporate & Securities, (iii) Trusts & Estates, (iv) Labor & Employment, (v) Tax[ation], (vi) Bankruptcy, (vii) Litigation, and (viii) Energy.<sup>139</sup> Over the last two years, the amount insurers are paying to settle claims has increased, as has the cost of defending legal malpractice cases. The reasonableness of law firm WFH and RTW policies will add another layer of complexity for a judge to weigh. This suggests that the cost of defending such cases, and if necessary, settling them, is likely to increase.<sup>140</sup>

The Ames & Gough study found: “Ninety percent of the insurers polled indicated the cost to defend legal malpractice claims increased in 2019. . . .

---

(Mar. 23, 2020, 10:37 AM), <https://www.law360.com/articles/1255561/virus-poses-latest-test-to-supporting-attys-mental-health> [<https://perma.cc/A2WR-HVM6>] (explaining the pandemic increased attorney stress and anxiety); *IBA Embarks on First Phase of Global Initiative on Mental Wellbeing in the Legal Profession*, INT'L BAR ASS'N (July 10, 2020), <https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=aef94ee7-38c9-49bd-aaa8-be1bbc2cf800> [<https://perma.cc/2ZZD3-TCPX>] (indicating the International Bar Association “embarked on a global project aimed at addressing the mental wellbeing of legal professionals as Covid-19 exacerbates tensions in professional and personal lives”).

137. Under the Rules, legal fees must be reasonable. Among the factors that may be considered in determining “reasonableness” are:

(1) [T]he time and labor required, the novelty and difficulty of the questions involved, and the skill requisite to perform the legal service properly; (2) the likelihood, if apparent to the client, that the acceptance of the particular employment will preclude other employment by the lawyer; (3) the fee customarily charged in the locality for similar legal services; (4) the amount involved and the results obtained; (5) the time limitations imposed by the client or by the circumstances; (6) the nature and length of the professional relationship with the client; (7) the experience, reputation, and ability of the lawyer or lawyers performing the services; and (8) whether the fee is fixed or contingent.

MODEL RULES OF PROF'L CONDUCT R. 1.5 (AM. BAR. ASS'N 2020).

138. See Robinson, *supra* note 136 (describing the stresses exacerbated by COVID-19); Coe, *supra* note 136 (describing the same).

139. Garczynski & Lessell, *supra* note 132, at 28.

140. See John Wynn & Rob Herchert, *The Impact of COVID-19 and the Potential Economic Downturn on Legal Malpractice Claims*, EPIC INS. BROKERS & CONSULTANTS (Oct. 20, 2020), <https://epicbrokers.com/insights/lemme-law-firm-best-practices-forum-recap> [<https://perma.cc/YJL4-TT2D>] (pointing out challenges related to COVID-19 that contribute to higher costs in defending claims).

Meanwhile, the hourly rates insurers pay defense counsel also continued to rise in 2019; 80% of the insurers polled saw rates increase [in 2019].”<sup>141</sup>

Using a different insurance-industry data set, the Lemme Law Firm, a subdivision of EPIC Insurance Brokers & Consultants, had the opportunity to compare the types of legal malpractice cases arising early during the pandemic in comparison with earlier years.<sup>142</sup> It identified certain types of claims law firms are expected to face, which are summarized below (some of which were mentioned above):<sup>143</sup>

- **Buyer’s Remorse Claims:** [C]lients want to get out of regrettable deals and [blame their outside counsel]. Firms with real estate practices are especially at risk due to failed transactions as a result of the current pandemic[.]<sup>144</sup>
- **Unworthy Clients:** [S]ome clients that were good clients at the time of [the initial] intake will become unworthy clients over time, particularly if they are struggling financially from the impact of COVID-19[.]<sup>145</sup>
- **COVID-19 Losers:** [C]ertain client sectors . . . have been particularly hard hit by COVID-19, including the hospitality and travel industries[.]<sup>146</sup>
- **Human Error:** [S]ignificant increase in claims from ‘sloppy’ lawyering in recent years[.] . . . that trend is likely to continue with more lawyers working remotely, dabbling in unfamiliar practice areas, and the inability to consult with their colleagues . . . .[.]<sup>147</sup>
- **Wrongful Foreclosure Claims [(especially due to government moratoriums)]:** Banks and their law firms getting sued for wrongful

---

141. AMES & GOUGH, LPLI 2020 CLAIMS SURVEY, *supra* note 134; see LEMME LAW FIRM PRAC. TEAM, *supra* note 132 (indicating insurers are seeking higher rates); Dan Packel, *Legal Malpractice Payouts Climb, and with COVID-19, No Crest in Sight*, AM. LAW. (May 26, 2020, 5:00 AM), <https://www.law.com/americanlawyer/2020/05/26/legal-malpractice-payouts-climb-and-with-covid-19-no-crest-in-sight> [<https://perma.cc/373R-87JN>] (referencing the Ames & Gough study); Joshua J.T. Byme, *Legal Malpractice and COVID-19: The Devil Is in the Details and Follow the Money*, LEGAL INTELLIGENCER (Mar. 27, 2020, 12:32 PM), <https://www.law.com/thelegalintelligencer/2020/03/27/legal-malpractice-and-covid-19-the-devil-is-in-the-details-and-follow-the-money> [<https://perma.cc/2EMH-8CA2>] (identifying basic items to concentrate on to avoid legal malpractice claims).

142. See Wynn & Herchert, *supra* note 140 (asking questions of a panel of industry experts related to potential COVID-19 malpractice claims).

143. *Id.*

144. *Id.*

145. *Id.*

146. *Id.*

147. *Id.*

foreclosure claims . . . . Collection firms are seeing an increase in claims[.]<sup>148</sup>

- **Poor Timing:** Labor and employment types of claims have increased as a result of counsel given at time of deciding furloughs, layoffs, etc. [(for example, age discrimination and other types of claims related to “protected groups”).]<sup>149</sup>
- **PPP [Paycheck Protection Program] Loans:** Claims arising out of counsel provided concerning PPP loan application and/or eligibility[; and]<sup>150</sup>
- **Force Majeure Challenges:** [The application of force majeure clauses is likely to be a major source of litigation. Clients may sue their law firms for not drafting suitable force majeure clauses.]<sup>151</sup>

According to Lemme’s surveys, the most severe losses for large and medium law firms will be in the securities, taxation, commercial transactions, and litigation practice areas.<sup>152</sup>

Lawyers and their law firms are more likely to commit legal malpractice if their personnel do not work in a systematic manner—for example, if there is inadequate supervision of junior lawyers and staff by the people who typically oversee them. After the outbreak of the pandemic, law firms may have thinned their ranks as a cost-cutting measure. Furthermore, remote supervisory efforts are not as effective as in-person supervision. These factors increase legal malpractice risk, and not surprisingly, can harm law firm cyber-hygiene.

## V. LAW FIRM CYBERSECURITY

Generally, cybersecurity is not directly regulated in the United States.<sup>153</sup> As noted by one of the leading specialists on cybersecurity and the law, Jeff

---

148. *Id.*

149. *Id.*

150. *Id.*

151. *Id.* The Lemme Law Firm Practice Team also released an earlier report identifying some causes of legal malpractice claims and the steps law firms should take to reduce their risk of committing legal malpractice in the post-pandemic environment. LEMME LAW FIRM PRAC. TEAM, *supra* note 132, at 5–6.

152. LEMME LAW FIRM PRAC. TEAM, *supra* note 132, at 3.

153. This statement is not intended to suggest that the federal government is unconcerned about private-sector cybersecurity and does not encourage and support private-sector cybersecurity efforts. See CISA Information & Updates on COVID-19, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, <https://www.cisa.gov/coronavirus> [<https://perma.cc/J7GW-HH9Z>] (outlining what the

Kosseff, the United States “does not have a single ‘cybersecurity law’ that . . . app[lies] to all circumstances.”<sup>154</sup> “Rather, the United States has a patchwork of hundreds of state and federal statutes, regulations, binding guidelines, and court-created rules regarding data security, privacy, and other issues commonly considered to fall under the umbrella of ‘cybersecurity.’”<sup>155</sup>

In the future, the forces driving law firms’ and other organizations’ cybersecurity regulation may be indirect; nonetheless, lawyers will need to comply with the rules governing their professional conduct and their contractual arrangements. Governmental entities are already starting to deputize the clients of law firms to ensure that the latter’s cybersecurity practices are sufficiently rigorous. For example, the New York Department of Financial Services’ Cybersecurity Regulations requires “covered entities” such as banks, insurance companies, and other financial service organizations to designate Chief Information Security Officers, adopt comprehensive cybersecurity programs, and develop and maintain “an ongoing reporting system for cybersecurity events.”<sup>156</sup>

In turn, these covered entities are required to conduct periodic risk assessments that, *inter alia*, evaluate their relationships with “third party service providers.”<sup>157</sup> Covered entities’ policies and procedures must set

---

government is doing about cybersecurity); *Cybersecurity Resources*, FDIC (July 27, 2021), <https://www.fdic.gov/regulations/resources/cybersecurity/> [https://perma.cc/T2LH-CY2H] (providing resource options for different individuals and institutions); *Coronavirus (COVID-19) Information for Bankers and Consumers*, FDIC (Jan. 13, 2021), <https://www.fdic.gov/coronavirus/index.html> [https://perma.cc/5YKM-6F3M] (presenting information on how “[t]he FDIC is working with federal and state banking agencies . . . [and] financial institutions” to help customers affected by the Coronavirus); *DHS Responds: Coronavirus (COVID-19)*, HOMELAND SEC. (July 29, 2021), <https://www.dhs.gov/coronavirus> [https://perma.cc/97XZ-6ARC] (explaining what the Department of Homeland Security has done to help with COVID-19). Under the existing regulatory regime, state governments are responsible for ensuring persons and organizations whose confidential and private data have been compromised due to a cyber-attack are properly notified. See *Security Breach Notification Laws*, *supra* note 117 (setting forth each state’s law that assigns notification responsibility). There is no United States equivalent to the General Data Protection Regulation (GDPR). See EUR. COMM’N, EUR. UNION, *EUROPEAN DATA GOVERNANCE* (2020), <https://ec.europa.eu/digital-single-market/en/news/data-governance-act> [https://perma.cc/VC4Q-9L2N] (showing Europe’s plan to manage data more safely).

154. JEFF KOSSEFF, *CYBERSECURITY LAW* xxi (2019).

155. *Id.*

156. Juliana De Groot, *What Is the NYDFS Cybersecurity Regulation? A Cybersecurity Compliance Requirement for Financial Institutions*, DIGIT. GUARDIAN (Dec. 1, 2020), <https://digitalguardian.com/blog/what-nydfs-cybersecurity-regulation-new-cybersecurity-compliance-requirement-financial> [https://perma.cc/UYW2-YVX2].

157. *Id.*

out “relevant guidelines for due diligence and/or contractual protections” concerning third party service providers, including law firms, addressing:

(1) [law firms’] policies and procedures for access controls, including [their] use of Multi-Factor Authentication . . . to limit access to relevant Information Systems and Nonpublic Information; (2) [law firms’] policies and procedures for use of encryption . . . to protect Nonpublic Information in transit and at rest; (3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity’s Information Systems or the Covered Entity’s Nonpublic Information being held by [law firms]; and (4) representations and warranties addressing [law firms’] cybersecurity policies and procedures that relate to the security of the Covered Entity’s Information Systems or Nonpublic Information.<sup>158</sup>

At the federal level, the Security and Exchange Commission and Congress have a growing interest in cybersecurity and are likely to compel the public to disclose certain data breaches, not merely information disclosed pursuant to state disclosure laws. In the future, publicly traded companies are likely to demand that their outside counsel improve their cybersecurity. If the law firms fail to secure their clients’ data, it will cause harm to their reputation and harm their bottom line.<sup>159</sup>

---

158. NY COMP. CODES R. & REGS. tit. 23, § 500.11(a)–(b) (2021); see *Cybersecurity Resource Center*, N.Y. STATE DEPT OF FIN. SERVS., [https://www.dfs.ny.gov/industry\\_guidance/cybersecurity](https://www.dfs.ny.gov/industry_guidance/cybersecurity) [<https://perma.cc/9TWX-KDTG>] (“All entities and persons regulated or licensed by the New York State Department of Financial Services are required to file various cybersecurity notices to the Superintendent.”); De Groot, *supra* note 156 (“Organizations must enact controls, including encryption of sensitive data, depending on the outcome of a risk assessment.”).

159. See Steve W. Klemash et al., *What Companies are Disclosing About Cybersecurity Risk and Oversight*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Aug. 25, 2020), <https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight> [<https://perma.cc/XW5R-TL3L>] (describing the cybersecurity threats and how they can harm a firm’s reputation and revenue); SEC OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS PUBLISHES OBSERVATIONS ON CYBERSECURITY AND RESILIENCY PRACTICES, U.S. SEC. & EXCH. COMM’N (Jan. 27, 2020), <https://www.sec.gov/news/press-release/2020-20> [<https://perma.cc/953B-FSKE>] (“The Securities and Exchange Commission Commission’s Office of Compliance Inspections and Examinations (OCIE) today issued examination observations related to cybersecurity and operational resiliency practices taken by market participants.”); OFF. OF COMPLIANCE INSPECTIONS & EXAMINATIONS, U.S. SEC. & EXCH. COMM’N, CYBERSECURITY AND RESILIENCY OBSERVATIONS 1, <https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf> [<https://perma.cc/9H72-3EZ2>] (discussing cybersecurity recommendations); Robert K. Knake, *Expanding Disclosure Policy to Drive Better Cybersecurity*, COUNCIL ON FOREIGN RELS. (Oct. 16, 2019), <https://www.cfrt.org/report/disclosure-policy-cybersecurity> [<https://perma.cc/5UVR-RNZT>] (“Threats to national and economic security emanating from cyberspace are all too real, but public disclosure of incidents of the theft of intellectual property (IP) is exceedingly rare.”); Rob Scott, *SEC Demands Better*

The scope of cybersecurity is considerably broader than the mere protection of the confidentiality, integrity, and availability (CIA) of data from non-violent, non-kinetic cyber-attacks by criminals. Potential harms include unauthorized access, alteration, destruction, disclosure, modification, or use of data by a third party by any means, including through an insider.

Although the United States government has a role in the defense of the private sector's cybersecurity, it is limited.<sup>160</sup> Indeed, nation-states, such as China, have conducted cyber-attacks against United States law firms,<sup>161</sup> and

---

*Disclosure for Cybersecurity Incidents and Threats*, HELP NET SEC. (Apr. 30, 2019), <https://www.helpnetsecurity.com/2019/04/30/sec-demands-better-disclosure-for-cybersecurity-incidents-and-threats/> [<https://perma.cc/4T8V-YRYE>] (identifying risks to be disclosed); Nathaniel Sobel, *The SEC and Cybersecurity Regulation*, LAWFARE (Nov. 19, 2018), [www.lawfareblog.com/sec-and-cybersecurity-regulation](http://www.lawfareblog.com/sec-and-cybersecurity-regulation) [<https://perma.cc/HH33-H7MT>] (“[T]he Securities and Exchange Commission (SEC) has, under its authority of enforcing the federal securities laws, steadily increased its regulation of cybersecurity-related matters.”).

160. See Jonathan Reiber & Benjamin Bahney, *The U.S. Government Can Deepen Its Operational Partnership with the Private Sector to Better Defend the U.S. in Cyberspace*, LAWFARE (Mar. 13, 2020, 4:06 PM), <https://lawfareblog.com/us-government-can-deepen-its-operational-partnership-private-sector-better-defend-us-cyberspace> [<https://perma.cc/8XU7-CU4P>] (examining the need for an enhanced cybersecurity public-private operational partnership); FIREYE, EVOLVING ROLE OF GOVERNMENT IN CYBER SECURITY 2 (2018), <https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/wp-evolving-role-gov.pdf> [<https://perma.cc/Q2CN-WATC>] (defining the role of the government in cybersecurity); Mary Calam et al., *Asking the Right Questions to Define Government's Role in Cybersecurity*, MCKINSEY & CO. (Sept. 19, 2018), <https://www.mckinsey.com/industries/public-and-social-sector/our-insights/asking-the-right-questions-to-define-governments-role-in-cybersecurity> [<https://perma.cc/NJ39-YECC>] (“In the United States, the Department of Homeland Security coordinates a national infrastructure-protection plan and requires sector-specific agencies to develop sector-specific plans.”); *Ensuring the Cybersecurity of the Nation*, U.S. GOV'T ACCOUNTABILITY OFF., <https://www.gao.gov/highrisk/ensuring-cybersecurity-nation> [<https://perma.cc/CUL8-2HB5>] (providing links to numerous government reports relating to cybersecurity, and observing that “[f]ederal agencies and other entities need to take urgent actions to implement a comprehensive cybersecurity strategy, perform effective oversight, secure federal systems, and protect cyber critical infrastructure, privacy, and sensitive data”); David Simon et al., *Legal Considerations Raised by the U.S. Cyberspace Solarium Commission Report*, LAWFARE (July 20, 2020), <https://www.lawfareblog.com/legal-considerations-raised-us-cyberspace-solarium-commission-report> [<https://perma.cc/H2YF-KK4A>] (evaluating the Cyberspace Solarium Commission Report and noting that there is no “federal statutory framework for establishing liability for security vulnerabilities in software, hardware or firmware,” and in its absence, “[t]he Federal Trade Commission (FTC)—as the primary regulator of cybersecurity practices that affect American consumers—enforces cybersecurity standards principally through its authority under Section 5 of the Federal Trade Commission Act, which prohibits ‘unfair’ and ‘deceptive’ practices against consumers”).

161. Dan Packel, *US Law Firm Falls Victim to Alleged Chinese Hacking as Clients Face Threats*, AM. LAW. (Feb. 20, 2019, 5:11 PM), <https://www.law.com/americanlawyer/2019/02/20/law-firms-still-a-great-target-as-us-firm-falls-victim-to-alleged-chinese-hack> [<https://perma.cc/6DC7-GT5T>].

made attempts to illegally acquire information related to COVID-19 vaccine efforts.<sup>162</sup> The forms of these attacks are essentially the same as those prior to the COVID-19 outbreak, but now many lawyers are working remotely with cybersecurity systems that were designed to be centralized in their principal offices where law firm personnel were less distracted than they are at home.<sup>163</sup>

Another (albeit less common) purpose of private-sector cybersecurity is the physical protection of an organization's property and persons.<sup>164</sup> Hence, cybersecurity should anticipate kinetic attacks against law firms to gain an advantage in litigation, market manipulation, and malware schemes. While financial gain obtained by monetizing data in some fashion is typically the motivation of cybercriminals, some may have other motives, such as furthering the interests of nation-states.<sup>165</sup>

---

162. Ellen Nakashima & Devlin Barrett, *U.S. Accuses China of Sponsoring Criminal Hackers Targeting Coronavirus Vaccine Research*, WASH. POST (July 21, 2020, 1:46 PM), [https://www.washingtonpost.com/national-security/us-china-covid-19-vaccine-research/2020/07/21/8b6ca0c0-cb58-11ea-91f1-28aca4d833a0\\_story.html](https://www.washingtonpost.com/national-security/us-china-covid-19-vaccine-research/2020/07/21/8b6ca0c0-cb58-11ea-91f1-28aca4d833a0_story.html) [<https://perma.cc/P99Q-6XYK>].

163. See Michael Coden et al., *Managing the Cyber Risks of Remote Work*, BCG (Mar. 20, 2020), <https://www.bcg.com/publications/2020/covid-remote-work-cyber-security> [<https://perma.cc/9Y7A-VC7E>] ("[S]hifting work patterns on such a massive scale can have serious unanticipated implications for IT and cybersecurity.").

164. See generally RICHARD A. CLARKE & ROBERT K. KNAKE, *THE FIFTH DOMAIN: DEFENDING OUR COUNTRY, OUR COMPANIES, AND OURSELVES IN THE AGE OF CYBER THREATS* (2019) (identifying cyber threats and examining how to defend against them); NATO COOP. CYBER DEF. CENT. OF EXCELLENCE, *TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS* (Michael N. Schmitt ed., 2d ed. 2017) (identifying international law governing cyber warfare and operations); MARTIN C. LIBICKI, *CYBERSPACE IN PEACE AND WAR* (2016) (covering international cyber law and related issues); MARC GOODMAN, *FUTURE CRIMES* (2015) (exploring recent advances in cyber threats); SHANE HARRIS, *@WAR: THE RISE OF THE MILITARY-INTERNET COMPLEX* (2015) (exploring policies and strategies for cybersecurity and managing cyber-conflict); HEATHER HARRISON DINNISS, *CYBER WARFARE AND THE LAWS OF WAR* (repr. ed. 2014) (discussing the dangers of technology hackers); *CYBERSECURITY: SHARED RISKS, SHARED RESPONSIBILITIES* (Peter M. Shane & Jeffrey Hunker eds., 2013) (examining cybersecurity from a military angle).

165. See Garrett Hinck & Tim Maurer, *Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity*, 10 J. NAT'L SEC. L. & POL'Y 525, 526 (2020), <https://jnslp.com/wp-content/uploads/2020/05/Criminal-Charges-as-a-Response-to-Nation-State-Malicious-Cyber-Activity.pdf> [<https://perma.cc/J9PG-97LP>] (questioning the efficacy of using transnational law enforcement mechanisms to pursue cyber-mercenaries acting at the behest of nation-states); see also MARK GALEOTTI, EUR. COUNCIL ON FOREIGN RELS., *CRIMINTERN: HOW THE KREMLIN USES RUSSIA'S CRIMINAL NETWORKS IN EUROPE* 1, 6 (2017), [https://www.ecfr.eu/page/-/ECFR208\\_-\\_CRIMINTERN\\_-\\_HOW\\_RUSSIAN\\_ORGANISED\\_CRIME\\_OPERATES\\_IN\\_EUROPE02.pdf](https://www.ecfr.eu/page/-/ECFR208_-_CRIMINTERN_-_HOW_RUSSIAN_ORGANISED_CRIME_OPERATES_IN_EUROPE02.pdf) [<https://perma.cc/S3NL-A97K>] ("Russian-based organized crime groups in Europe have been used for a variety of purposes, including as sources of 'black cash', to launch cyber

### A. Reducing Law Firm Vulnerability to Cyber-Attacks

Many law firms are discovering that they are particularly vulnerable to insider-attack schemes, in part, because lawyers have a long history of working autonomously without regard to their colleagues' activities.<sup>166</sup> It is essential that law firms monitor their IT and communication networks to identify potential insider threats.<sup>167</sup> The type of information needed by law firms to monitor personnel, manage workflow, and ascertain productivity is not the same as is needed for cybersecurity purposes (though the data collected in many respects may be similar).

---

attacks, to wield political influence, to traffic people and goods, and even to carry out targeted assassinations on behalf of the Kremlin.”).

166. See Victoria Hudgins, *Who's Responsible for Preventing Insider Cyber Threats? Depends Who You Ask*, LEGALTECH NEWS (Dec. 18, 2020, 9:00 AM), <https://www.law.com/legaltechnews/2020/12/18/whos-responsible-for-preventing-insider-cyber-threats-depends-who-you-ask> [https://perma.cc/DS7C-6MHL] (asking, administratively, who within a law firm should have primary responsibility for combating the insider threat); Andrew McDermott, *How to Protect Your Law Firm From Insider Threats*, BILL4TIME (Feb. 3, 2020), <https://www.bill4time.com/blog/how-to-protect-your-law-firm-from-insider-threats> [https://perma.cc/V3KB-6DCN] (discussing how to develop a strategy to reduce insider threat risk); *A Guide to Data Security for Law Firms*, EMBROKER (Jan. 29, 2021), <https://www.embroker.com/blog/cybersecurity-for-law-firms/> [https://perma.cc/H5TM-LCCT] (providing a valuable guide targeted at insider threat issues within law firms); Jennifer Detrani, *An Inside Look at Insider Threats (Part I)*, ABOVE THE L. (May 2, 2019), <https://abovethelaw.com/2019/05/an-inside-look-at-insider-threats> [https://perma.cc/5CMP-X458] (offering tips for preventing insider-threat attacks); Jennifer Detrani, *An Inside Look at Insider Threats (Part II)*, ABOVE THE L. (May 16, 2019), <https://abovethelaw.com/2019/05/an-inside-look-at-insider-threats-part-2> [https://perma.cc/WF62-F3BZ] (providing a look at motivations and preventive measures); OPENTEXT, THE THREAT FROM WITHIN: HOW LAW FIRMS AND CORPORATE LEGAL DEPARTMENTS ARE BOLSTERING SECURITY POSTURES TO PROTECT SENSITIVE DATA 3 (2021), [https://www.opentext.com/file\\_source/OpenText/en\\_US/PDF/opentext-insider-threats-white-paper.pdf](https://www.opentext.com/file_source/OpenText/en_US/PDF/opentext-insider-threats-white-paper.pdf) [https://perma.cc/YAX4-8SVW] (“[Forty-eight] percent of law firms had been subject to a data security audit at the behest of at least one corporate client over the preceding year.”); Debra Juhnke, *Law Firm Insider Threats Don't Take a Break for the Holidays—They May Get Worse.*, INFO. GOVERNANCE GRP. LLC (Nov. 28, 2018), <https://www.informationbytes.com/2018/11/law-firm-insider-threats-dont-take-break-holidays-may-get-worse> [https://perma.cc/6WMX-J2U3] (discussing a range of warning signs and measures to reduce vulnerability); Jordan McQuown, *The Six Biggest Inside Threats to Law Firm IT*, SEC. BOULEVARD (Mar. 27, 2018), <https://securityboulevard.com/2018/03/the-six-biggest-inside-threats-to-law-firm-it> [https://perma.cc/2ETR-73ZD] (discussing the results of a LogicForce survey of more than 300 law firms regarding insider threats).

167. For a description of a network security monitoring system, see *AT&T Cybersecurity Insights™ Report: 5G and the Journey to the Edge*, AT&T CYBERSECURITY, <https://cybersecurity.att.com/resource-center/white-papers/cybersecurity-insights-report-tenth-edition> [https://perma.cc/4FGJ-P7FF]; IBM Security Products, IBM, <https://www.ibm.com/security/products> [https://perma.cc/9T92-UZDE].

Personnel monitoring is especially important when a significant share of the law firm personnel is working remotely.<sup>168</sup> The monitoring of personnel for cybersecurity purposes has a counter-espionage flavor. The system should perform a range of functions such as keeping track of the individual's actions, identifying what networks and files are being accessed, what websites are being visited, the nature of external communications, and what computer files are being downloaded.<sup>169</sup>

Law firms, like other organizations, have two principal duties with respect to data security: (i) a duty to protect data and (ii) a duty to disclose "to affected parties and regulators" in the event of a data breach.<sup>170</sup> Law firms represent a tempting target for cybercriminals because:

- (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.<sup>171</sup>

It is doubtful that cybercriminals will ever lose their interest in attacking law firms.

---

168. See, e.g., *Guide to Securing Organizational Changes in the New Remote Work Reality*, CODE42, <https://www.code42.com/resources/article-guide-to-securig-organizational-changes-in-the-new-remote-work-reality/> [<https://perma.cc/4BY9-CB8G>] ("[W]hile [remote workers] are all focused on getting their work done, what might not be so apparent is that they are also opening up their companies to heightened data risk.").

169. See, e.g., *Remote Desktop and Employee Monitoring Solutions*, DESKGATE IT SERV., <https://www.deskgate.com/en/default> [<https://perma.cc/4MCX-8P42>] (describing functions of one type of personnel monitoring software).

170. Ruth Hill Bro, *Cybersecurity 101*, in STANDING COMM. ON L. & NAT'L SEC. ET AL., AM. BAR ASS'N, REMOTE WORKING IN A TIME OF COVID-19: CYBERSECURITY ISSUES YOU NEED TO KNOW 8, 14 (2020), [https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2020/mar/cs2020\\_0092.pdf](https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2020/mar/cs2020_0092.pdf) [<https://perma.cc/JQ3X-B2AD>].

171. David G. Ries, 2018 *Cybersecurity*, ABA (Jan 28, 2019), [https://www.americanbar.org/groups/law\\_practice/publications/techreport/ABATECHREPORT2018/2018Cybersecurity](https://www.americanbar.org/groups/law_practice/publications/techreport/ABATECHREPORT2018/2018Cybersecurity) [<https://perma.cc/G6EQ-WM7Z>] (discussing ABA Formal Opinion 477); ABA Comm. on Ethics & Prof. Resp., Formal Op. 477R, at 2 (2017), [https://www.americanbar.org/content/dam/aba/administrative/professional\\_responsibility/aba\\_formal\\_opinion\\_477.pdf](https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf) [<https://perma.cc/UD3V-39UV>]. Professor Eli Wald identified a third factor worth noting—that law firms may feel pressured by clients or competitors to adopt technology before it might be advisable from an operational standpoint. Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19 CHAP. L. REV. 501, 503–04 (2016).

In 2012, the ABA formed its Cybersecurity Task Force drawing on expertise found throughout the ABA.<sup>172</sup> Subsequently, the ABA amended its Rules (the amendments collectively known as the “Technology Amendments”),<sup>173</sup> printed more than 400 articles,<sup>174</sup> produced podcasts, organized CLE sessions and conferences, printed books, and issued Formal Opinions<sup>175</sup>—all related to myriad aspects of cybersecurity.<sup>176</sup> It is indisputable that law firms that fail to observe a reasonable standard of care are opening themselves up to potential legal malpractice claims. Although there are not many reported decisions by courts in this area, the wealth of material produced by the ABA, particularly the *ABA Cybersecurity Handbook*,

---

172. THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS xv (Jill D. Rhodes & Robert S. Litt eds., 2d ed. 2018).

173. *Model Rules of Professional Conduct - Table of Contents*, ABA, [https://www.americanbar.org/groups/professional\\_responsibility/publications/model\\_rules\\_of\\_professional\\_conduct/model\\_rules\\_of\\_professional\\_conduct\\_table\\_of\\_contents](https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents) [https://perma.cc/2THY-467P]; see J.S. “Chris” Christie Jr., *Tort Trial and Insurance Practice: What Should an Ethical Lawyer Know About Technology?*, ABA (May/June 2017), [https://www.americanbar.org/groups/gpsolo/publications/gp\\_solo/2017/may-june/tort-trial-insurance-practice-what-should-ethical-lawyer-know-about-technology](https://www.americanbar.org/groups/gpsolo/publications/gp_solo/2017/may-june/tort-trial-insurance-practice-what-should-ethical-lawyer-know-about-technology) [https://perma.cc/6P94-Q9D2] (explaining the Technology Amendments, including changes to Model Rules 1.1 *Competence* and 1.6 *Confidentiality of Information*, as well as relevant risks); see also Conor M. Shankman, *Cyberattacks Have Become Commonplace – Know the Ethics of Prevention and Response*, ABA (Aug. 16, 2019), [https://www.americanbar.org/groups/construction\\_industry/publications/under\\_construction/2019/summer/respond-to-cyberattacks](https://www.americanbar.org/groups/construction_industry/publications/under_construction/2019/summer/respond-to-cyberattacks) [https://perma.cc/3ECS-H827] (“Opinion No. 483 interprets and applies the 2012 Technology Amendments to the Model Rules of Professional Conduct . . .”).

174. See generally *Cybersecurity*, ABAJOURNAL, <https://www.abajournal.com/topic/cybersecurity> [https://perma.cc/JMR9-7SBC] (showing 443 cybersecurity articles published by the *ABA Journal* as of August 4, 2021). See Sharon D. Nelson & John W. Simek, *Hot Buttons A Road Map for Lawyers with Cybersecurity Paralysis*, ABA (July/Aug. 2019), [https://www.americanbar.org/groups/law\\_practice/publications/law\\_practice\\_magazine/2019/JA2019/JA2019HotButtons](https://www.americanbar.org/groups/law_practice/publications/law_practice_magazine/2019/JA2019/JA2019HotButtons) [https://perma.cc/SJ28-3C6G] (sharing views of leading specialists offering a useful and manageable description of the problem of cybersecurity management inertia); Julie Sobowale, *Law Firms Must Manage Cybersecurity Risks*, A.B.A. J., Mar. 2017, at 34, 34–36 [https://www.abajournal.com/magazine/article/managing\\_cybersecurity\\_risk](https://www.abajournal.com/magazine/article/managing_cybersecurity_risk) [https://perma.cc/VHL8-NYXX] (addressing cybersecurity issues as they pertain to law firms as a whole as well as client-specific risks).

175. See generally ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R (2017), [https://www.americanbar.org/content/dam/aba/administrative/professional\\_responsibility/aba\\_formal\\_opinion\\_477.pdf](https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf) [https://perma.cc/UD3V-39UV] (regarding the securing of protected client information); ABA Comm. on Ethics & Pro. Resp., Formal Op. 483 (2018), [https://www.americanbar.org/content/dam/aba/images/news/formal\\_op\\_483.pdf](https://www.americanbar.org/content/dam/aba/images/news/formal_op_483.pdf) [https://perma.cc/4GM8-GBYS] (explaining “[l]awyers’ [o]bligations [a]fter an [e]lectronic [d]ata [b]reach or [c]yberattack”).

176. See *Cybersecurity Legal Task Force*, ABA, <https://www.americanbar.org/groups/cybersecurity/> [https://perma.cc/GV5T-QVVT] (explaining the ABA Journal series “Digital Dangers” explores “[c]yber topics lawyers need to know, from practice management tips on cyber-insurance to questions about decrypting digital evidence”).

goes far in establishing best practices within the legal profession that are important both for legal malpractice and cybersecurity purposes.<sup>177</sup>

According to the FBI, reported cybercrime quadrupled at the onset of the COVID-19 pandemic.<sup>178</sup> Lawyers, law firms, and their staff are particularly vulnerable to cyber-attacks for several reasons. Working remotely has forced them to use new devices and follow new procedures that are unfamiliar. Since they are working in new environments, they are encountering new patterns online, such as instructions from individuals with whom they have not interacted in the past (e.g., IT professionals). They may click on messages that purport to share new procedures or pandemic-related information from public health or governmental authorities that on their face might seem benign. Also, for a variety of reasons, they may be distracted when working remotely from home, particularly if they are concerned that the law firms for whom they work might not need their services in the future.<sup>179</sup>

Such personnel are particularly susceptible to specific types of attacks (e.g., credential phishing, malicious attachments and links, business email compromise, malware, ransomware, and engineering opportunities).<sup>180</sup>

---

177. *But cf.* Robert Hilson, *This Article on Lawyer Cybersecurity Will Scare You Out of a Malpractice Suit*, LOGIKCULL (June 10, 2016), <https://www.logikcull.com/blog/paper-lawyer-cybersecurity-will-scare-malpractice-suit> [<https://perma.cc/8CMG-DSY5>] (indicating there is much more the ABA can do to further establish best practices).

178. Catalin Cimpanu, *FBI Says Cybercrime Reports Quadrupled During COVID-19 Pandemic*, ZDNET (Apr. 18, 2020), <https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic> [<https://perma.cc/B5LL-B68W>]; see also Leonardas Marozas, *We Need to Rethink Cybersecurity for a Post-Pandemic World. Here's How*, WORLD ECON. F. (Aug. 13, 2020), <https://www.weforum.org/agenda/2020/08/rethink-cybersecurity-post-pandemic-world/> [<https://perma.cc/KGR3-RSZU>] (noting “the cybersecurity community has observed numerous attack vectors that use a COVID-19 theme either as bait or as a way to conceal malicious activity from easy identification and detection”); Michael Daniel et al., *How Do We Beat COVID-19 Cybercrime? By Working Together*, WORLD ECON. F. (July 6, 2020), <https://www.weforum.org/agenda/2020/07/alliance-tackling-covid-19-cybercrime> [<https://perma.cc/ELB6-GEUM>] (calling for more private-sector partnering among “cyber-related service and platform providers, multinational financial organizations, government agencies, international organizations and leading non-for-profit alliances”).

179. See Victoria Hudgins, *Prepare for Slower Data Breach Detection, Higher Costs with Remote Workforce*, LEGALTECH NEWS (Aug. 10, 2020, 10:30 AM), <https://www.law.com/legaltechnews/2020/08/10/prepare-for-slower-data-breach-detection-higher-costs-with-remote-workforce> [<https://perma.cc/J3R2-RDZN>] (indicating working remotely increases problems connected with “data incident monitoring and compliance”).

180. Ransomware represents the greatest external threat to law firms. See Danny Palmer, *Ransomware vs WFH: How Remote Working is Making Cyberattacks Easier to Pull Off*, ZDNET (Oct. 27, 2020), <https://www.zdnet.com/article/ransomware-vs-wfh-how-remote-working-is-making-cyberattacks-easier-to-pull-off> [<https://perma.cc/4DUV-L3UB>] (“[R]ansomware attacks have

Remote operations degrade law firm cyber-defenses, as they were designed largely for office-based work.<sup>181</sup> The reduced effectiveness of law firms' remote surveillance of their networks is reflected in higher dwell times.

Cybersecurity training demands that employees are aware of their roles as envisioned by law firms' security policies, procedures, standards, and guidelines. It should be more than a minimalist "security awareness"

---

become even more pervasive—and effective during the course of this year."); Staci Zaretsky, *Global Biglaw Firm Hit By 'Aggressive' Ransomware Attack*, ABOVE THE L. (Oct. 12, 2020), <https://abovethelaw.com/2020/10/global-biglaw-firm-hit-by-aggressive-ransomware-attack> [https://perma.cc/Q793-CPFP] ("Given the highly sensitive data that Biglaw firms deal with on an everyday basis, cybersecurity is of the utmost importance—especially during unprecedented times like these when entire firms are doing work remotely."); Casey C. Sullivan, *Ransomware Hits Law Firms Hard—And It's Worse Than Ever Before*, LOGIKCULL (Mar. 5, 2020), <https://www.logikcull.com/blog/maze-ransomware-law-firms> [https://perma.cc/HY8P-K6JE] ("This latest evolution of ransomware attacks is being driven by a new form of ransomware known as Maze. A typical Maze attack works similarly to a normal ransomware attack: The victim's network is infiltrated and its information encrypted or otherwise seized."); Mark Sangster, *What Every Firm Needs to Know About Mitigating Cultural Engineering Attacks During M&A*, LEGALTECH NEWS (Oct. 30, 2020, 7:00 AM), <https://www.law.com/legaltechnews/2020/10/30/what-every-firm-needs-to-know-about-mitigating-cultural-engineering-attacks-during-ma> [https://perma.cc/R6XA-K23F] ("Large legal firms are at particular risk for ransomware and cultural engineering, given the highly confidential nature of the data they have on file and the number of employees able to access it."); Sharon D. Nelson & John W. Simek, *Ten Cybersecurity Lessons Learned About Working From Home*, SENSEI ENTERS, INC. (2020), <https://senseienterprises.com/wp-content/uploads/WFH-Cybersecurity-Lessons.pdf> [https://perma.cc/U4TQ-WF9Q] (providing a list of ten work-from-home cybersecurity suggestions); Phil Muncaster, *Maze Ransomware Hits Law Firms and French Giant Bouygues*, INFOSECURITY GRP. (Feb. 3, 2020), <https://www.infosecurity-magazine.com/news/maze-ransomware-law-firms-french> [https://perma.cc/Y6GE-Q9YK] ("Cyber-criminals behind the Maze ransomware attacks have claimed several more scalps over the past few days, including five law firms and a French industrial giant, all of which are thought to have had sensitive internal data stolen."); Joe Patrice, *The Ransomware Attack on Your Firm Is Coming and You're Probably Not Prepared*, ABOVE THE L. (June 18, 2018), <https://abovethelaw.com/2018/06/the-ransomware-attack-on-your-firm-is-coming-and-youre-probably-not-prepared> [https://perma.cc/T5GX-9XYF] ("But today, the easiest assault on a computer system is ransomware—a debilitating attack where an anonymous belligerent forces you to pay them to get your system back.").

181. Cf. Tom Spiggle, *Can Employers Monitor Employees Who Work from Home Due to the Coronavirus?*, FORBES (May 21, 2020), <https://www.forbes.com/sites/tomspiggle/2020/05/21/can-employers-monitor-employees-who-work-from-home-due-to-the-coronavirus/?sh=1e6d0d122fb7> [https://perma.cc/LXX6-VD6U] (asserting most states permit employers the right to monitor what their employees do while working from home "as long as it's for legitimate business purposes," is done in a reasonable manner, and the employees consent); Reid Blackman, *How to Monitor Your Employees—While Respecting Their Privacy*, HARV. BUS. REV. (May 28, 2020), <https://hbr.org/2020/05/how-to-monitor-your-employees-while-respecting-their-privacy> [https://perma.cc/328R-BVDU] (urging employers to not overdo their efforts to monitor their workers working remotely); Bobby Allyn, *Your Boss Is Watching You: Work-From-Home Boom Leads to More Surveillance*, NPR (May 13, 2020), <https://www.npr.org/2020/05/13/854014403/your-boss-is-watching-you-work-from-home-boom-leads-to-more-surveillance> [https://perma.cc/9PH2-D2GX] (discussing ways employers monitor their employees).

program. Cybersecurity training should not be divorced from the work regime. It should require employees to report instances of their colleagues' non-compliance with cybersecurity requirements to appropriate cybersecurity personnel and result in the imposition of sanctions against employees who fail to comply with security policies and procedures.<sup>182</sup> Such sanctions might include shaming, being put on leave without pay, or termination.

Lawyers may be cyber-savvy without necessarily being specialists in cybersecurity law. One can become a specialist in cybersecurity by taking individual courses and earning specialized certificates. Persons who want to build up a practice in cybersecurity should consider enrolling in one of many LL.M. programs, which are often offered online.<sup>183</sup>

It is important that law firms educate their staff on confidentiality issues to better appreciate the risk of data breaches.<sup>184</sup> "Regular training for employees about these and other 'do's and don'ts' can help avoid a large number of potential data breaches within law firms."<sup>185</sup>

Law firm training should make use of lectures, role-playing exercises, simulations, and videos, to cover topics such as:

- Accessing websites and rules involving online communications;

---

182. See generally Thomas J. Smedinghoff & Ruth Hill Bro, *Lawyers' Legal Obligations to Provide Data Security*, in THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS, *supra* note 172, at 85–86.

183. See Leonard Wills, *How to Become a Cybersecurity Lawyer*, ABA (Nov. 2, 2018), <https://www.americanbar.org/groups/litigation/committees/minority-trial-lawyer/practice/2018/how-to-be-come-a-cybersecurity-lawyer> [<https://perma.cc/4GNZ-95HJ>] (suggesting steps like taking an IT course, IT training, and obtaining IT certifications); see also 10 Best Cyber Security Courses [2021 August Updated], DIGITALDEFYND (Aug. 2021), <https://digitaldefynd.com/best-cyber-security-courses-and-training-online/> [<https://perma.cc/T3E5-ZBXY>] (containing a compilation "of Best Cyber Security Courses, Training, Bootcamp Certifications, Classes and Tutorial available online for 2021"); Online Cybersecurity Certification Programs, CYBERSECURITY GUIDE (Aug. 6, 2021), <https://cybersecurityguide.org/online/cybersecurity-certifications/> [<https://perma.cc/36NC-SB9A>] ("For people that already have a degree or work experience in the space, then certification programs provide fantastic vehicles for advancing careers by keeping industry knowledge current."); Steven Bowcut, *Guide to a Cybersecurity Law Degree*, CYBERSECURITY GUIDE (Feb. 25, 2021), <https://cybersecurityguide.org/programs/cybersecurity-law> [<https://perma.cc/7J2T-KMU9>] ("The main focus of this guide will be the LL.M. degree with a concentration in cybersecurity.").

184. See CNA, CYBER-SAVVY LAWYERS: SMART CYBER PRACTICES IN LAW FIRMS 6 (2016), <https://www.cna.com/web/wcm/connect/15944804-e35c-46bf-b7d1-25b2233edb83/Small-Business-Content-Whitepaper.pdf?MOD=AJPRES> [<https://perma.cc/4JMF-YHR2>] (suggesting training can reduce the likelihood of a data breach).

185. *Id.*

- Cloud storage of data;
- Encryption;
- Knowing one's role with respect to antivirus, spam, firewalls, and spyware protection;
- Password management;
- Physical security of one's work area;
- Protecting clients' personal identifiable information (PII);
- Social media etiquette and related risks;
- Spotting potential attacks by cybercriminals and managing uncertainty;
- Steps to take to redress a data breach, including notification of clients, relevant government authorities, and third parties;
- Understanding the function of one's law firms' IT and communication systems components and the monitoring thereof;
- Use of virtual private networks (VPNs);
- Vulnerabilities created by bringing your own device (BYOD); and
- Working with law enforcement.<sup>186</sup>

Training should be an ongoing process with a formal session done annually or semi-annually.<sup>187</sup> To the extent appropriate, the person(s) responsible for cybersecurity management should inform all law firm personnel of significant cybersecurity incidents on a regular basis or immediately, if deemed necessary. Law firm personnel should be notified in writing of any changes to cybersecurity policies, procedures, and practices. Law firm

---

186. See generally *id.* (outlining issues that should be covered in a training program). See Dave Coffey, *Cybersecurity: Tips for Attorneys*, LAW TECH. TODAY (Oct. 23, 2018), <https://www.lawtechnologytoday.org/2018/10/cybersecurity-tips-for-attorneys> [https://perma.cc/CN6Z-ZLEZ] (discussing cybersecurity tips generally and advocating training); Sharon D. Nelson & John W. Simek, *Security Awareness Training for Law Firm Employees*, SENSEI ENTERS, INC. (2016), <https://senseient.com/wp-content/uploads/Security-Awareness-Training-for-Law-Firm-Employees.pdf> [https://perma.cc/FYY2-UBKN] (suggesting content for law firm security awareness programs).

187. See Nelson & Simek, *supra* note 186 (indicating law firms should require training “[at least annually”]).

personnel should be tested regarding these changes and other cybersecurity issues every few months.<sup>188</sup>

### B. Principle vs. Rule-Based Cybersecurity

To ensure their compliance with their ethical obligations, lawyers must observe “reasonable” cybersecurity practices.<sup>189</sup> Of course, reasonable people will disagree about what this entails. Unfortunately, lawyers and their law firms may be unwilling or unable to afford to implement a uniformly high standard of cybersecurity for all their clients due to cost and efficiency concerns.<sup>190</sup>

Most cybersecurity specialists advocate that law firms should use a risk-based cybersecurity framework based on that developed by NIST, the ISACA COBIT 2019 Framework,<sup>191</sup> or ISO 2700.<sup>192</sup> Risk-based cybersecurity is usually set out in the form of best practices.<sup>193</sup> Risk-based cybersecurity is also known as “principle-based” cybersecurity.<sup>194</sup> The principles tend to be generally worded and therefore are said to have the

---

188. See *id.* (suggesting firms hire outside trainers to send employees fake emails to test whether they can spot the potential risk).

189. See MODEL RULES OF PROF'L CONDUCT R. 1.1 (AM. BAR ASS'N 2020) (“Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”); *Id.* at R. 1.1 cmt. 8 (“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 . . .”).

190. Cf. Coffey, *supra* note 186 (“It’s no surprise that the firms surveyed cited balancing security with usability, user acceptance and behavior, and user education and awareness as the top three biggest law firm security challenges.”).

191. The Information Systems Audit and Control Association has been rebranded and now goes by its acronym—ISACA COBIT 2019. *COBIT Effective IT Governance at Your Fingertips*, ISACA, <https://www.isaca.org/resources/cobit> [<https://perma.cc/JWX4-W2UC>].

192. ISO/IEC 27032:2012(en) *Information Technology—Security Techniques—Guidelines for Cybersecurity*, ISO, <https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:en> [<https://perma.cc/M9VB-4G2M>]; *Cybersecurity Framework*, NIST, <https://www.nist.gov/cyberframework> [[perma.cc/27DZ-4K26](https://perma.cc/27DZ-4K26)].

193. See Ryan Blanch, *REvil's Lessons: It's Time Law Firms Quit Taking Cybersecurity for Granted*, SEC. BOULEVARD (June 6, 2020), <https://securityboulevard.com/2020/06/revils-lessons-its-time-law-firms-quit-taking-cybersecurity-for-granted> [<https://perma.cc/M5K4-C9VN>] (explaining why, when preparing for data breaches, law firms should consider hiring cybersecurity firms or retaining counsel to advise on best cybersecurity practices).

194. See Edward R. McNicholas et al., *CFTC Issues Cybersecurity Rules on System Safeguards Testing Requirements*, FUTURES & DERIVATIVES L. REP., Oct. 2016, at 1, 4 (“Although the Final Rules specify particular types of testing, for other matters, such as frequency and scope, they defer to a Covered Entity’s ‘appropriate risk analysis,’ providing Covered Entities with some flexibility as to how they conduct their testing.”).

advantage of being flexible—something that may be advantageous in the uncertainties of the post-COVID-19 world.<sup>195</sup>

There are also “rule-based cybersecurity” advocates. Rule- or “compliance-based” cybersecurity is designed to comply with set regulations, rules, or other norm-setting standards often set out in the form of checklists. In theory, they offer the advantage of simplicity, appropriate to be used by persons who are not cybersecurity specialists. Typically, the checklists do not permit much discretion or flexibility appropriate for the relevant organization’s needs—their value is to identify areas where action needs to be taken.<sup>196</sup> Unfortunately, the lists may hide complexities demanding further consideration due to unanticipated circumstances.

These models often result in “Goldilocks and the Three Bears” solutions. This entails starting with the risk-based approach to develop a baseline for adding appropriate rules consistent with the organization’s needs and risk tolerance.<sup>197</sup> Here, the risk and rule-based approaches are only diametrically opposed in theory, while in practice, they are complementary.<sup>198</sup> Consequently, it should not be a surprise that many

---

195. See *id.* at 1, 4 (explaining the principles-based approach in CFTC’s Final Rules provides flexibility).

196. Daniel Garrie and Bill Spernow have generated a useful set of principles law firms should observe when developing their cybersecurity efforts. See generally DANIEL B. GARRIE & BILL SPERNOW, LAW FIRM CYBERSECURITY (2017). These principles are organized into their “Ten Commandments of Cybersecurity”:

[(i)] Develop and Practice Strong Cyber Hygiene[, (ii)] Know and Secure Vendors’ Networks[, (iii)] Identify and Protect the ‘Crown Jewels’[, (iv)] Practice Your Incident Response Plan[, (v)] Create and Develop a Global Communication and Messaging Framework[, (vi)] Test the Incident Response Plan and Update Regularly[, (vii)] Develop a Robust Cyber Threat Monitoring and Sharing Team[, (viii)] Evaluate Cyber Insurance[, (ix)] Engage Privacy and Cybersecurity Expertise for All Priority Jurisdictions[, and (x)] Maintain Government Relationships.

*Id.* Of course, law firms apply these principles in a manner consistent with their profile. Under each Commandment is practical advice on a range of cybersecurity topics, such as “A Survey of Cyber Threats and Their Context,” “What it Takes to Frustrate the Hacker Knocking at Your Door,” and “How Law Firms May Use the Cybersecurity Framework for Critical Infrastructure.” *Id.* at 15–17, 20–39, 40–55, 94–118; see *A Guide to Data Security for Law Firms*, *supra* note 166 (noting lawyers are targets for cyber-attacks and that firms must be careful of this risk).

197. See *What Does Your IAM Spending Look Like?*, FORMMI INC. (Sept. 28, 2020), <https://www.formmi.com/post/what-does-your-iam-spending-look-like> [https://perma.cc/ED99-2TUJ] (promulgating a list of factors to be considered to create the right fit for cybersecurity risk assessments).

198. See Wei Chen Lin & Dominic Saebeler, *Risk-Based v. Compliance-Based Utility Cybersecurity—A False Dichotomy?*, 40 ENERGY L.J. 243, 245 (2019) (suggesting risk and rule-based approaches can lead to greater benefits by balancing flexibility with minimum levels of security).

organizations—law firms, in particular—adopt a hybrid approach using aspects of each “pure approach.”<sup>199</sup>

The hybrid approach may be appropriate for law firms that may use a principle-based scheme for organizing their own data, and a compliance system consistent with the manner in which their clients organize their data. Data takes many forms such as: personal information of employees, customers or clients, and prospects; business or client financial information; tax information; trade secrets; and other confidential information. Law firms must ensure the protection of media storage devices, such as flash drives, laptops, CDs, DVDs, cellphones, their computer systems, networks (both in-house and in the cloud), and communications sharing such data.<sup>200</sup>

### C. Law Firm Best Cybersecurity Practices

Even before the additional challenges posed by COVID-19, there was a debate over the extent to which the legal community would be willing to follow best cybersecurity practices given the resulting costs and inefficiencies. As noted by Denver University Sturm College of Law Professor Eli Wald, “some lawyers, notwithstanding their awareness of cybersecurity threats, fail to take reasonable steps to protect themselves and their clients, because they are underregulated, likely to escape any meaningful consequences for their inaction, and therefore, have little incentive to take reasonable cybersecurity action.”<sup>201</sup>

---

199. See Steven T. Kroll, *Security Governance Framework: The Hybrid Approach*, CYBERCRIME MAG. (June 25, 2019), <https://cybersecurityventures.com/security-governance-framework-the-hybrid-approach/> [https://perma.cc/J9BM-UMH7] (discussing the former White House CIO, Ms. Theresa Payton, recommending a hybrid approach to cybersecurity); *How to Protect Your Law Firm from Ransomware in 2020*, BLANCH L. FIRM, <https://www.theblanchlawfirm.com/how-to-protect-your-law-firm-from-ransomware-in-2020/> [https://perma.cc/4RTY-WGC7] (listing solutions law firms should consider to prevent a cyber attack); *How to Protect Your Companies from Rising Cyber Attacks and Fraud Amid the COVID-19 Outbreak*, PWC (Aug. 11, 2020), <https://www.pwc.com/us/en/library/covid-19/cyber-attacks.html> [https://perma.cc/XHV9-M6N9] (suggesting simulated attacks to keep employees prepared to fight cyber-attacks); *Cyber Security for Law Firms—7 Critical Objectives for 2021*, ATLANT SEC. (2020), <https://atlantsecurity.com/cybersecurity-for-law-firms/> [https://perma.cc/PV3Z-PC27] (discussing cyber threats to law firms and items to consider related to cyber-defenses).

200. Ruth Hill Bro & Jill D. Rhodes, *Get SMART on Data Protection: Training and How to Create a Culture of Awareness*, in THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS, *supra* note 172, at 271, 274 (indicating these physical mediums must be secured regardless of how strong the IT security policy is because these physical devices can still be compromised).

201. Wald, *supra* note 171, at 501–02. In most cases, lawyers do not face disciplinary or legal malpractice claims for failing to observe good cybersecurity practices. Furthermore, lawyers are not

Perhaps law firm cybersecurity practices should be inspired and even judged by standards contained in a document released by the International Bar Association (IBA) in October 2018.<sup>202</sup> The IBA Presidential Task Force on Cyber Security's Cyber Security Guidelines are a comprehensive and well-organized cybersecurity planning tool suitable for most law firms. It is written in language that is readily understandable to persons who are not cybersecurity specialists. After the outbreak of the pandemic, the IBA's Technology Law Committee recognized that COVID-19 required that law firms change the manner by which they operate, necessitating revisions in the Cyber Security Guidelines.

Ultimately, on June 11, 2020, the IBA Technology Law Committee released the "IBA cybersecurity guidelines for law firms during the Covid-19 crisis."<sup>203</sup> The massive migration by law firms to online and remote operations led to greater exposure to the "risk of ransomware attacks, malware attacks and phishing emails," than previously appreciated, as well as an increase in "challenges posed by cyber stalkers who are exploiting the increased flow of internet-enabled communications (Internet of Things)."<sup>204</sup> "The intersection points transmitting the flow of data in

---

required to report all instances of data breaches to their clients, regulators, or relevant third parties unless required by contract or law. As a result, lawyers generally "do not face market sanctions, such as being fired or suffering reputational losses." *Id.* at 502. *See generally* ABA Comm. on Pro. Ethics & Resp., Formal Op. 477R (2017). This situation might change if the Rules were to be modified to provide for mandatory reporting by lawyers of their colleagues' improper or reckless cybersecurity conduct. *See generally* Arthur F. Greenbaum, *The Attorney's Duty to Report Professional Misconduct: A Roadmap for Reform*, 16 GEO. J. LEGAL ETHICS 259 (2003) (noting the importance of mandatory reporting of ethics rules in a self-regulating profession).

202. *See Cyber Security Guidelines*, INT'L BAR ASS'N (Oct. 2018), <https://www.ibanet.org/LPRU/cybersecurity-guidelines.aspx> [<https://perma.cc/2R3A-4R5B>] (highlighting the importance of the effective use of cybersecurity technologies). The IBA established the "Presidential Task Force on Cyber Security" for the purpose of:

[(i)] producing a set of recommended best practices to help law firms to protect themselves from breaches of data security; [(ii)] assisting their ability to keep operations running if a breach of data security or ransom attack does occur; [(iii)] giving their clients the best possible assurances that their data is protected; [and (iv)] helping protect the reputation of the profession.

*Id.*

203. Anurag Bana, *IBA Cybersecurity Guidelines for Law Firms During the Covid-19 Crisis*, INT'L BAR ASS'N (June 11, 2020), <https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=25FA3B61-C5EE-4EB7-A987-5C795B911DCD> [<https://perma.cc/RHD4-U5A9>].

204. *Id.*

multiple interoperable devices can challenge the security of the devices because of the changing structure and architecture of networks.”<sup>205</sup>

The IBA-revised cybersecurity guidelines recognizes the cybersecurity challenges arising from operating in the post-pandemic environment and that, although lawyers are “outside of a conventional office space[, that] does not necessarily exclude or excuse the lawyers from their fundamental duty of making all efforts in keeping all communications and data confidential.”<sup>206</sup> Videoconferencing can be particularly vexing in light of the risk of “uninvited attendees” exploiting “private unprotected link[s] in the public domain.”<sup>207</sup>

There is a tone underpinning the IBA Guidelines that “basic” or “standard” cybersecurity safeguards can be obtained without a substantial financial investment or operational disruption. It is not clear whether this assumption is valid in the face of motivated and skilled cybercriminals.

Perhaps, some of the non-financial benefits of cyber-insurance in the form of advice may help law firms to focus their attention on achieving better cyber-hygiene by designing and implementing appropriate cybersecurity policies, practices, and procedures. Indeed, there may be genuine benefits to law firms choosing to undergo thorough underwriting merely to obtain appropriate cybersecurity planning documents as part of the cyber-insurance procuring process, whether they decide to purchase insurance or not. The same type of planning documents may be obtained as a deliverable part of cybersecurity risk assessments from qualified consultancies. Nonetheless, law firm management may not be able to reach a consensus on how to respond to the recommendations they receive. Still, having an external cybersecurity police officer to defer to (or blame) may have its benefits if law firm leadership is not willing to make tough and unpopular decisions involving the expenditure of funds for uncertain gains, particularly when revenues are low.

## VI. CYBER-INSURANCE

While the topic of cybersecurity insurance is largely outside the scope of this Article, some observations are in order since COVID-19 has implications for various insurance-related topics, including business interruption, health (both private and public), legal malpractice, and

---

205. *Id.*

206. *Id.*

207. *Id.*

cybersecurity.<sup>208</sup> Not surprisingly, the insurance industry, consultancies, law firms, and to a lesser extent, federal and state governmental bodies have generated the lion's share of the published materials examining cyber-insurance.<sup>209</sup> Except for established virtual law firms, most law firm cybersecurity programs were not designed for situations where a large share of the firm is working remotely. Most of the cyber-insurance literature takes the view that cyber-insurance is essential for law firms, which is not surprising since much of it was done to promote the sale of cyber-insurance and related services.<sup>210</sup> At times it seems that some governmental and

---

208. See Brian Haney, *How to Assess Your Insurance Coverage Amid the COVID-19 Crisis*, ASAE (May 4, 2020), [https://www.asaecenter.org/resources/articles/an\\_plus/2020/may/how-to-assess-your-insurance-coverage-in-the-wake-of-covid-19](https://www.asaecenter.org/resources/articles/an_plus/2020/may/how-to-assess-your-insurance-coverage-in-the-wake-of-covid-19) [https://perma.cc/E3MA-8RP2] (emphasizing the need for law firms to evaluate all their insurance measures); Gary Shaw, *Potential Implications of COVID-19 for the Insurance Sector*, DELOITTE (Mar. 18, 2020), <https://www2.deloitte.com/us/en/insights/economy/covid-19/impact-of-covid-19-on-insurers.html> [https://perma.cc/47SG-VUTZ] (discussing the challenges for insurers and the industry in addressing the impacts of COVID-19).

209. See *Cyber Insurance*, FED. TRADE COMM'N, <https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/cyber-insurance> [https://perma.cc/R5TD-7WKS] (listing a variety of resources to understand cybersecurity insurance); SASHA ROMANOSKY ET AL., RAND INST. FOR CIV. JUST., CONTENT ANALYSIS OF CYBER INSURANCE POLICIES 8, [https://www.ftc.gov/system/files/documents/public\\_events/1223263/panel012\\_cyberinsurance\\_policies.pdf](https://www.ftc.gov/system/files/documents/public_events/1223263/panel012_cyberinsurance_policies.pdf) [https://perma.cc/L6CG-XRSU] (describing important factors to consider when choosing a cyber-insurance policy).

210. See Karen M. Kroll, *Cybersecurity Insurance Is a Must Have'for Law Firms*, A.B.A.J., Nov. 2016, at 31, 31, [https://www.abajournal.com/magazine/article/data\\_breach\\_insurance\\_coverage](https://www.abajournal.com/magazine/article/data_breach_insurance_coverage) [https://perma.cc/E69J-RDH4] (suggesting cybersecurity insurance is a "must have" for law firms); *Cyber Liability Insurance—Checklist for Law Firms*, USI AFFINITY (June 22, 2020), <https://insurance.focus.usiaffinity.com/2020/06/cyber-liability-insurance-checklist-for-law-firms.html> [https://perma.cc/6WC2-ZX8M] (advising law firms to consider cyber-insurance as part of an overall cybersecurity approach with the continuation of a work from home environment); Gregg Wirth, *More Law Firms Are Buying Cyber Insurance, But not All*, AON (June 2020), <https://www.aon.com/risk-services/professional-services/more-law-firms-are-buying-cyber-insurance.jsp> [https://perma.cc/AQG9-2Y5M] (noting an increase from around six out of 300 firms to nearly 60% of firms purchasing cyber-insurance in recent years); *Professional Services Practice Cyber Risk*, AON (2020), <https://www.aon.com/risk-services/professional-services/cyber-risk-cyber-insurance.jsp> [https://perma.cc/VAG2-93V3] (providing a strategic approach for a comprehensive cybersecurity policy); Edward M. Dunham, Jr., *Getting Full Insurance Coverage for Your Actual Cyber Exposures: A Users' Guide to the Nut and the Grit*, ABA (Feb. 20, 2020), [https://www.americanbar.org/groups/business\\_law/publications/blt/2020/03/cyber-expenses](https://www.americanbar.org/groups/business_law/publications/blt/2020/03/cyber-expenses) [https://perma.cc/74ZE-PM3Z] (listing essential steps to follow when acquiring cyber-insurance); *Law*, EMBROKER, <https://www.embroker.com/industry/law-firm> [https://perma.cc/JJW7-ATVC] (noting the benefits of a cyber-insurance policy). *But see* Jason Tashea, *Are You Covered? Cyber Insurance Market Is Highly Unstable and Lacks Uniformity*, A.B.A.J., June 2018, at 30, 31, [https://www.abajournal.com/magazine/article/coverage\\_cyber\\_insurance\\_market](https://www.abajournal.com/magazine/article/coverage_cyber_insurance_market) [https://perma.cc/A2TS-ZCVW] (discussing certain coverage gaps under cyber-insurance).

legislative bodies see themselves as partisan promoters of cyber-insurance as well.<sup>211</sup>

Most lawyers in private practice have professional liability (legal malpractice) policies.<sup>212</sup> A majority of these policies are likely to decline coverage to lawyers who fail to provide reasonable cybersecurity. Whether lawyers should purchase cyber-insurance requires a careful analysis of the potential insureds' needs and the particulars of the insurance policies being evaluated.<sup>213</sup>

The Ponemon Institute's "Cost of a Data Breach Report 2020" puts the average total cost of a data breach at \$3.86 million.<sup>214</sup> It is not clear that

---

211. See Mariam Baksh, *Federal Contractors Argue Cyber Insurance Isn't a Safe Bet for Better Security*, NEXTGOV (Oct. 14, 2020), <https://www.nextgov.com/cybersecurity/2020/10/federal-contractors-argue-cyber-insurance-isnt-safe-bet-better-security/169231/> [<https://perma.cc/6LZ7-DW3N>] (illustrating "the government's role facilitating coverage of cybersecurity risks"); Nour Aburish et al., *The Role of Cyber Insurance in Securing the Private Sector*, FOUND. FOR DEF. OF DEMOCRACIES (Sept. 13, 2019), <https://www.fdd.org/analysis/2019/09/11/cyber-insurance> [<https://perma.cc/XW79-T9TV>]; *Cybersecurity Insurance*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, <https://www.cisa.gov/cybersecurity-insurance> [<https://perma.cc/629H-SWFZ>] (defining cybersecurity insurance and its design); Andrew G. Simpson, *U.S. Cybersecurity Report Calls for Major Government Role in Cyber Insurance*, INS. J. (Mar. 11, 2020), <https://www.insurancejournal.com/news/national/2020/03/11/560918.htm> [<https://perma.cc/4MBM-54QZ>] (reporting on the need for cyber-insurance).

212. Susan Saab Fortney, *Mandatory Legal Malpractice Insurance: Exposing Lawyers' Blind Spots*, 9 ST. MARY'S J. ON LEGAL MALPRACTICE & ETHICS 190, 235 (2019).

213. See generally Eileen R. Garczynski, *Protecting Against Cyber Threats: A Lawyer's Guide to Choosing a Cyber Liability Insurance Policy* (2d. ed. 2020), <https://www.americanbar.org/products/inv/book/385016340> [<https://perma.cc/33EC-CG64>] (describing how to "assist firms in making an informed decision about selecting cyber liability insurance"); *Cyber Liability Insurance*, HOLLAND & KNIGHT, <https://www.hklaw.com/en/services/practices/technology-and-cybersecurity/cyber-liability-insurance> [<https://perma.cc/SNK2-W87E>] (advising law firm clients when "evaluating, negotiating and enforcing their cyber liability insurance policies"); *Cyber Insurance*, LAWS. INS. GRP., <https://lawyersinsurer.com/cyber-insurance> [<https://perma.cc/R4W3-3T3F>] (noting "[s]tandard property, general liability and crime policies will [generally] not cover damage to or loss of intangible assets such as data and systems" arising from cyber-attacks, but that business owners' policies, comprehensive general liability, and legal malpractice insurance policies may cover such harm because of cyber-attacks in certain circumstances).

214. David Atkinson, *What Does a Data Breach Cost in 2020?*, SENSEON BLOG (2020), <https://www.senseon.io/blog/cost-of-a-data-breach-in-2020> [<https://perma.cc/WDX4-4WH8>] (representing the figure for the average cost across industries for a data breach is \$3.86 million and referring to the Ponemon Study for IBM); see also *Cybersecurity Services*, IBM, <https://www.ibm.com/security/services> [<https://perma.cc/7B63-NDNN>] (providing a link to the "2021 Cost of a Data Breach Report"). Discussions about the cost of cyber-attacks against law firms need to be dealt with gingerly. They are a product of law firm size, revenue, practice sector, cybersecurity policies, practices, and procedures. See Emily Mossburg et al., *Beneath the Surface of a Cyberattack: A Deeper Look at Business Impacts*, DELOITTE, <https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html> [<https://perma.cc/7BUL-29XN>]

this average figure is of much analytical use to a law firm for planning purposes (as opposed to the “median” value—the mid-point in a set, or the mode—the most frequent amount).

The above-discussed data about law firms having cyber-insurance reflect the fact that the ABA Survey includes many solo practitioners and small firms. In a 2015 press release, ALM Intelligence seems to indicate that two-thirds of U.S. law firms had cyber-insurance, but that statistic must have been a misstatement.<sup>215</sup> U.S. corporations tend to retain larger U.S. law firms. The Association of Corporate Counsel’s Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information requires that outside counsel have cyber-insurance in an amount not less than ten million dollars.<sup>216</sup> This is a relatively small amount given the possibility of significant law firm liability as a result of data breaches and other claims. It suggests that law firms with large clients should consider procuring cybersecurity insurance in greater amounts.<sup>217</sup>

Cyber-insurance policies, and cyber threats, have evolved well beyond data breaches to include coverage for fraudulent funds transfers and

---

(demonstrating the high risks of cyber-attacks); *Cost of a Data Breach*, FIREYE, <https://www.fireeye.com/current-threats/cost-of-a-data-breach.html> [https://perma.cc/BDR8-MLL7] (providing “questions will help qualify and quantify the cost” of a breach); *Who Is Responsible When a Data Breach Occurs?*, ERI BLOG (Feb. 4, 2019), <https://eridirect.com/blog/2019/02/who-is-responsible-when-a-data-breach-occurs> [https://perma.cc/ZNB2-BFMB] (discussing law firm liability for data breaches, as well as data breach responses and mitigation costs); *2020 Data Breach Investigations Report*, VERIZON, <https://enterprise.verizon.com/resources/reports/dbir> [https://perma.cc/8TRW-WKP3] (presenting data related to breach investigation and offering recommendations on cybersecurity—information from 2020 may be found by utilizing the Permalink, and information from 2021 may be found by utilizing the main website link).

215. The relevant highlight of the ALM Legal Intelligence Report was that “Approximately one-third of law firms do not hold cyber liability insurance policies.” *Cybersecurity Ignorance Is Big Risk for Law Firms & Corporate Counsel*, ALM Legal Intelligence Analysis Find, ALM (Dec. 16, 2015), [https://www.alm.com/press\\_release/cybersecurity-ignorance-is-big-risk-for-law-firms-corporate-counsel-alm-legal-intelligence-analysts-find](https://www.alm.com/press_release/cybersecurity-ignorance-is-big-risk-for-law-firms-corporate-counsel-alm-legal-intelligence-analysts-find) [https://perma.cc/WK4K-BAFH].

216. ASS’N OF CORP. COUNS., MODEL INFORMATION PROTECTION AND SECURITY CONTROLS FOR OUTSIDE COUNSEL POSSESSING COMPANY CONFIDENTIAL INFORMATION 10 (2017), [https://www.acc.com/sites/default/files/resources/advocacy/1454057\\_1.pdf](https://www.acc.com/sites/default/files/resources/advocacy/1454057_1.pdf) [https://perma.cc/3J4U-XLW9].

217. *Id.* Many small-to-medium law firms procure one million-dollar cyber-insurance policies, perhaps to allow them to tell existing or potential clients that they have cyber-insurance. See Shawn Moynihan et al., *Law Firms and Cyber Insurance: Under-Educated and Overexposed*, LAW.COM (July 23, 2018, 12:30 AM), <https://www.law.com/2018/07/23/law-firms-and-cyber-insurance-under-educated-and-overexposed/?slreturn=20210120154547> [https://perma.cc/2P3Y-P4W9] (showing the potential liability firms may face when they are not properly informed on cyber-insurance).

ransomware demands, insider threats, and technology failures, among many other forms of loss. Many law firms work with insurance companies to design their own cyber policies, practices, and procedures to incorporate into their insurance contracts as part of their effort to procure cyber-insurance on favorable terms. However, the best cybersecurity systems are of limited value if law firm personnel are not trained to operate remotely.<sup>218</sup>

As part of their application process, law firms typically complete detailed surveys along with their cybersecurity policies, procedures, and practices.<sup>219</sup> To obtain robust coverage, law firms must undergo cybersecurity risk assessments or audits.<sup>220</sup> Together along with the survey, the risk assessments form part of “baselines,” the deviation from which might form the basis for denials of claims.<sup>221</sup> It may prove problematic for law firms whose baselines do not envision higher levels of remote operations to successfully lodge claims under their cyber-insurance policies. Given the increased amount of cyber-attacks law firms are experiencing, law firms’ assumptions made at the time they acquired their policies may not be consistent with the threat profiles they currently face.

It is telling that despite the many proponents of standalone cyber-insurance, according to the most recent 2020 ABA Survey, only 36% of respondents purchased cyber-insurance even though its cost has remained relatively constant.<sup>222</sup> The 2019 ABA Survey put the figure at 33%, and the

---

218. As of June 2020, only two states had adopted mandatory “tech” (i.e., cybersecurity) CLE. Bob Ambrogi, *Another State Moves Closer to Mandating Tech CLE, but Limited to Cybersecurity*, LAWSITES (July 2, 2020), <https://www.lawsitesblog.com/2020/07/another-state-moves-closer-to-manding-tech-cle-but-limited-to-cybersecurity.html> [https://perma.cc/4E8Q-T6YV] (reporting how Florida and North Carolina have such a requirement, while Maine and New York are actively considering it).

219. Loughnane, *supra* note 112.

220. See George Grachis, *Law Firms Subject to Same Cyber Risk as Others, but Is Compliance Required?*, CSO (Jan. 4, 2017, 10:18 AM), <https://www.csionline.com/article/3154094/law-firms-subject-to-same-cyber-risk-as-others-but-is-compliance-required.html> [https://perma.cc/AS7E-XP5F] (“Once the risk assessment is complete, the consultant will be able to customize a program to fit the needs of the organization.”).

221. See *id.* (describing an example of a “blueprint” of a cybersecurity plan that may be designed for a law firm upon completion of a risk assessment).

222. Loughnane, *supra* note 112. But see Grachis, *supra* note 220 (sharing data on law firms without cyber-insurance and stating “[a]pproximately one-third of firms do not hold cyber liability insurance policies”). The cost of cyber-insurance seems to be trending upward by 5–10% due to the increase in ransomware claims. ADVISEN & PARTNERRE, CYBER INSURANCE—THE MARKET’S VIEW., 14 (2020), <https://partnerre.com/wp-content/uploads/2020/09/Cyber-Insurance-The-Markets-View-2020.pdf> [https://perma.cc/RT2Z-RQQY].

2018 ABA Survey indicated it was 34%.<sup>223</sup> One of the reasons that the take-up rate for cyber-insurance by law firms is not greater may be because insurance policies are often “limited to attacks and unauthorized activity, [and not] . . . accidental errors and omissions.”<sup>224</sup> As a result, “when deciding whether or not to pay out on a claim, an insurance company could simply point to a factor like human error” or deviation from the law firm’s cybersecurity baseline, which was submitted as part of the insurance application process, “and refuse to pay out the claim for a hacked computer system.”<sup>225</sup> It should be noted that after the COVID-19 outbreak, there seems to be more interest in cyber-insurance, particularly due to the increase in cybercrime. It remains to be seen if more law firms will choose to purchase such policies despite the “gaps.”<sup>226</sup>

---

223. Loughnane, *supra* note 112. These differences in take-up rates are statistically insignificant. They also do not account for law firms who purchased standalone cyber-insurance policies and those who added a “cyber” endorsement to an existing policy. For a discussion of the benefits of adding a cyber-endorsement to a standard property insurance policy see Cyber Insurance—The Market’s View. See generally ADVISEN & PARTNERRE, *supra* note 222 (reporting on the findings of a cybersecurity survey in one study).

224. Nicole Lindsey, *Businesses Are Finding Out That Cyber Insurance Coverage Might Not Be What They Thought*, CPO MAG. (Jan. 31, 2019), <https://www.cpomagazine.com/cyber-security/businesses-are-finding-out-that-cyber-insurance-coverage-might-not-be-what-they-thought> [<https://perma.cc/954Z-F2UJ>].

225. *Id.*; see John G. Buchanan & Marialuisa S. Gallozzi, *Kicking the Tires on a New Cyber Policy: Top Tips and Traps*, ABA (Jan. 22, 2018), <https://www.americanbar.org/groups/litigation/committees/insurance-coverage/articles/2017/cyber-policy-tips-traps> [<https://perma.cc/5Z66-G5WJ>] (recommending those searching for a cyber-insurance policy should “[r]eject ‘human error’ exclusions”). Rather than rely on cyber-insurance to manage their risks, law firms are increasing their investment in cybersecurity hardware, software, and expert advice. See L.S. Howard, *Business Cyber Losses Soar but Firms Fight Back with Extra Security Spending* Study, INS. J. (June 23, 2020), <https://www.insurancejournal.com/news/international/2020/06/23/573182.htm> [<https://perma.cc/DH5H-AWQ2>] (reporting on the high cyber losses).

226. See Gregg Wirth, *Forum Magazine: More Law Firms Are Buying Cyber Insurance, But Not All*, THOMSON REUTERS (June 3, 2020), <https://www.legalexecutiveinstitute.com/forum-magazine-spring-2020-cyber-insurance> [<https://perma.cc/PS3V-XRSE>] (noting, *inter alia*, the drop in the cost of cyber-insurance); Louis Columbus, *2020 Roundup of Cybersecurity Forecasts and Market Estimates*, FORBES (Apr. 5, 2020, 6:39 PM), <https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/#334ae6c1381d> [<https://perma.cc/FPR7-CGJ7>] (discussing cybersecurity threats, the quality of defenses, and the cyber-insurance market); Buchanan & Gallozzi, *supra* note 225 (analyzing several factors to consider for a cyber-insurance policy); Peter A. Halprin et al., *United States: Cybersecurity Insurance for Law Firms*, MONDAQ (Oct. 11, 2019), <https://www.mondaq.com/unitedstates/insurance-laws-and-products/850820/cybersecurity-insurance-for-law-firms> [<https://perma.cc/7H3P-S37S>] (warning, *inter alia*, of gaps “in coverage as currently written and interpreted by insurance companies—including the ‘direct loss’ defense invoked in crime policies, as well as the ambiguities in the terms of coverage for investigations and enforcement actions”); Thomas Ritter, *ABA Warns Lawyers That Data Breaches Raise Ethical Issues*, THOMPSON |

Cyber-insurance policies have been criticized for not being sufficiently standardized,<sup>227</sup> resulting in the cyber-insurance market being described by some as immature.<sup>228</sup> This lack of maturity translates into some difficulty for insurance companies when calculating premiums and anticipating payouts.<sup>229</sup> This situation is understandable given uncertainty about how these policies will operate and the lack of experience with the product and concomitant data, which exists for other traditional insurance products such as homeowners and automobile insurance.<sup>230</sup> As a result, many law firms

---

BURTON (Mar. 1, 2019), <https://thompsonburton.com/cybersecurity-law/2019/03/01/aba-warns-lawyers-data-breaches> [https://perma.cc/9V42-5SM7] (noting the ethical responsibilities lawyers have to clients in the event of a data breach); Bryce Friedman & Nick Goldin, *Leveraging Cyber Insurance to Mitigate the Economic Impact of Cyber Incidents*, N.Y. L.J. (May 8, 2020, 2:30 PM), <https://www.law.com/newyorklawjournal/2020/05/08/leveraging-cyber-insurance-to-mitigate-the-economic-impact-of-cyber-incidents> [https://perma.cc/L88S-JP88] (discussing the increased harm inflicted by cyber-attacks and the growing demand for cyber-insurance); Tashea, *supra* note 210 (noting cyber-insurance covers some gaps found in legal malpractice insurance).

227. In 2017, the National Association of Insurance Commissioners released its Insurance Data Security Model Law to promote the appearance of standard cyber-insurance policies, which would produce more predictable outcomes for both the insurance companies and insureds. NAT'L ASS'N OF INS. COMM'R'S, INSURANCE DATA SECURITY MODEL LAW 1 (2017), <https://content.naic.org/sites/default/files/inline-files/MDL-668.pdf> [https://perma.cc/T3UF-WUWA].

228. See James Bobotek, *10 Tips for Negotiating Your Cyber Insurance Policy*, ASAE (Apr. 24, 2018), [https://www.asaecenter.org/resources/articles/an\\_plus/2018/april/10-tips-for-negotiating-your-cyber-insurance-policy](https://www.asaecenter.org/resources/articles/an_plus/2018/april/10-tips-for-negotiating-your-cyber-insurance-policy) [https://perma.cc/GT9G-8TBP] (offering recommendations for negotiating a cyber-insurance policy); *Cyber Insurers Are Profitable Today, but Wary of Tomorrow's Risks*, BEST'S MKT. SEGMENT REP. (June 17, 2019), [https://reaction.ambest.com/reaction/emsdocuments/Special%20Reports/2019/2019.06\\_Cyber\\_Insurance\\_Report.pdf](https://reaction.ambest.com/reaction/emsdocuments/Special%20Reports/2019/2019.06_Cyber_Insurance_Report.pdf) [https://perma.cc/DE8J-2A28] (demonstrating the growth in cyber-insurance premiums); Heidi Roberts, *2020 Market Conditions Report: Private/Nonprofit D&O*, GALLAGHER (Oct. 26, 2020), <https://www.aig.com/us/news-and-insights/2020/feb/2020-market-conditions-report-private-nonprofit-d-o> [https://perma.cc/LE9S-NLRY].

229. See JOHN FARLEY, GALLAGHER, THE 2021 CYBER INSURANCE MARKET CONTINUES TO HARDEN 4 (2021), <https://www.aig.com/us/-/media/files/gallagher/us/news-and-insights/2021-q1-cyber-insurance-market-update.pdf> [https://perma.cc/BJ9Y-N5KJ] ("There is evidence of primary [insurance] markets looking to avoid specific industry sectors that they previously pursued. Even excess carriers are taking a cautious approach by offering lower limits than they may have in recent years. We expect cyber insurers to seek greater protection from the reinsurance market, which may in turn seek out protection for its own potential losses from the retrocession insurance market."). One interpretation of the aforementioned statement is that law firms are likely to encounter greater difficulty in lodging successful insurance claims or face higher premiums if the reinsurance market's fear of potential exposure from cyber-insurance continues to grow.

230. See Judy Greenwald, *Cyber Policies' Language Still Not Standardized*, BUS. INS. (Feb. 7, 2019, 10:06 AM), <https://www.businessinsurance.com/article/20190207/NEWS06/912326585/Cyber-policy-language-not-standardized-Professional-Underwriting-Liability-Socie> [https://perma.cc/FJK5-TVA2] (showing how difficult it can be for a single cyber-insurance policy to cover everything given the dynamic nature of cyber-attacks and defense against them).

have opted to self-insure or accept vulnerability to cyber-attacks as a cost of doing business.

Unlike publicly traded companies, law firms do not have a governance structure where officers and directors might act defensively to avoid accusations of negligence by shareholders. In addition, law firms tend to be thinly capitalized when compared to companies; that is, they lack sizeable reserve funds in their budgets that can be used to settle lawsuits, pay damages to plaintiffs, or cover attorney's fees when seeking to resolve disputes.

## VII. SOME TAKEAWAYS

At the pandemic's outset, it was anticipated that overall demand for legal services would drop, except possibly for certain law firms with niche practices.<sup>231</sup> While the second quarter of 2020 did see a drop in demand, many larger law firms found the decrease was not as severe as anticipated, and revenue in some of the largest law firms even grew during the first half of the year, topping revenue for the same time period in 2019.<sup>232</sup>

Perhaps these law firm revenue increases were a result of changes in billing practices, since overall demand was largely flat.<sup>233</sup> It might be explained by law firm partners and other senior lawyers doing work formerly performed by associates, a fact having ethical implications.<sup>234</sup>

---

231. See Debra Cassens Weiss, *More Work Shifted to Law Partners as Demand for Legal Services Dropped, New Report Says*, ABAJOURNAL (Aug. 13, 2020, 2:11 PM) [hereinafter Cassens Weiss, *More Work Shifted*], <https://www.abajournal.com/news/article/more-work-shifted-to-law-partners-as-demand-for-legal-services-dropped-report-says> [https://perma.cc/V7PL-4YAG] (noting a drop of 5.9% in demand for legal work); Todd Stager, *Demand for Legal Services Is Declining*, SEO FOR LAWS. (Nov. 9, 2020), <https://www.seo-for-lawyers.com/demand-for-legal-services-is-declining> [https://perma.cc/UDC9-QRHL] (explaining the decrease in demand for legal services over recent history). Law firms specializing in areas directly related to the pandemic, such as qualifying for government benefits, probably found a greater demand for their services.

232. See generally *The 2020 Am. Law 100*, AM. LAW. (2020), <https://www.law.com/americanlawyer/rankings/the-2020-am-law-100/> [https://perma.cc/2DDC-ZXWY] (reflecting on the 2020 AM LAW 100 survey and rankings of law firms by gross revenue, revenue per partner, profits per equity partner, and other data).

233. See Cassens Weiss, *More Work Shifted*, *supra* note 231 (explaining the change in demand and the concurrent shift in work to partners).

234. Patrick Smith, *Partners' Gain Is Associates' Pain as Hours Move Upstream*, AM. LAW. (Aug. 13, 2020, 5:00 AM), <https://www.law.com/americanlawyer/2020/08/13/partners-are-taking-a-larger-share-of-available-work-during-pandemic-and-that-has-consequences-for-associates> [https://perma.cc/RRY7-YWQ4]; MODEL RULES OF PROF'L CONDUCT R. 1.5 (AM. BAR. ASS'N 2020); see Patrick Smith, *Overall Demand Down for Big Law, But Rate Growth Hits All-Time High. Why?*, THERECODER (Aug. 10, 2020, 4:19 PM), <https://www.law.com/therecoder/2020/08/10/overall-demand-for-big>.

While there was an overall decline in lawyer productivity during the outset of the pandemic, roughly 70% of the respondents (120 firms) to a survey by Wells Fargo Private Bank, indicated their revenue for the first three-quarters of 2020 increased, even though "there's evidence of a steadily growing gap between the haves and the have-nots," with the former getting a bulk of the "high-end" work.<sup>235</sup> It seems that many law firms with established clients in certain practice areas such as "bankruptcy and financial restructuring, litigation, and finance and capital markets activity" have largely escaped the downturn in the legal services market.<sup>236</sup> In some cases, certain law firms found that "austerity measures," including first trimming staff followed by laying off associates, resulted in greater profitability.<sup>237</sup>

What of the future of remote law firm operations? After several months of shelter-in-place, a survey by Cushman & Wakefield's Global Legal Sector

---

law-is-down-but-rate-growth-hit-an-all-time-high-why-403-53442 [https://perma.cc/Q4ZS-VHVZ] (showing high rates during the COVID-19 pandemic); Debra Cassens Weiss, *BigLaw Partner Who Said She Worked 3,173 Billable Hours Is Suspended for Overbilling*, ABAJOURNAL (Dec. 16, 2019, 2:52 PM) [hereinafter Cassens Weiss, *BigLaw*], https://www.abajournal.com/news/article/biglaw-partner-who-said-she-worked-3173-billable-hours-is-suspended-for-overbilling [https://perma.cc/33Rj-HCND] (discussing overbilling prior to the pandemic).

235. Packel, *supra* note 7.

236. HILDEBRANDT CONSULTING LLC & CITI PRIV. BANK, 2021 CLIENT ADVISORY 3 (2021), https://www.privatebank.citibank.com/ivc/docs/2021CitHildebrandtClientAdvisory.pdf [https://perma.cc/LKM2-KHHJ]. A Hildebrandt Consulting LLC/Citi Private Bank Report states:

Am Law 1-50 firms fared better than other market segments in terms of demand performance, seeing a 0.2% drop in demand, compared with a 1.3% decline for Am Law 51-100 firms and 1.9% declines for Am Law Second Hundred firms and firms outside of the Am Law 200. While these segments trailed Am Law 1-50 firms in revenue growth, they achieved greater expense reductions, helping to protect, if not widen, their margins. Inventory growth was strong for all segments, suggesting that if firms are able to collect during the fourth quarter, we are likely to see a decent year-end as an industry average across all segments.

*Id.* at 6–7.

237. Debra Cassens Weiss, *Cuts in Lawyer Head Count and Expenditures 'Buoyed Profitability Metrics' at Law Firms, Report Says*, ABAJOURNAL (Nov. 11, 2020, 3:57 PM), https://www.abajournal.com/news/article/cuts-in-lawyer-headcount-and-expenditures-buoyed-profitability-metrics-at-law-firms-report-says [https://perma.cc/GPY4-47QE]; Debra Cassens Weiss, *Many BigLaw Firms are Quietly Laying Off Staff Members, Recruiters Say*, ABAJOURNAL (Oct. 28, 2020, 9:30 AM), https://www.abajournal.com/news/article/many-biglaw-firms-are-quietly-laying-off-staff-members-recruiters-say [https://perma.cc/7GSV-8E3J]. According to Cushman & Wakefield's Legal Sector Advisory Group's Benchmark and Associate Survey, 11% of the law firms surveyed in late 2020 hope to increase their profitability through downsizing or "careful attorney/staff evaluation." SHERRY CUSHMAN ET AL., CUSHMAN & WAKEFIELD, BRIGHT INSIGHT: THE 2020 NATIONAL LEGAL SECTOR BENCHMARK SURVEY RESULTS 4 (2020), https://www.cushmanwakefield.com/en/united-states/insights/2020-bright-insight [https://perma.cc/GJ2A-F4U3].

Advisory Group, consisting of over 350 advisors, found that “almost all respondents (90%) believe more than 10% of attorneys will work remotely on a regular basis.”<sup>238</sup> In the near term, remote operations combined with personnel reductions is likely to have a negative impact on most law firms’ efficiency and, ultimately, revenue.

Remote operations should lessen informal communications among lawyers within law firms and with clients, opposing counsel, judicial officials, etc., that might otherwise be expected, particularly given the requirement that communications might have to be encrypted. Such communications will need to be scheduled and instructions shared, but this does not eliminate the concern that some participants or even third parties may fear that unidentified persons may be overhearing the conversation. This concern may have an impact on mutual trust, an important intangible to resolve disputes or clarify uncertainties.

Indeed, greater supervision and monitoring of lawyers working remotely comes with possible pitfalls<sup>239</sup> and genuine costs. Under these circumstances, without law firms establishing management systems with greater accountability by lawyers to one another, as well as stricter oversight by clients, this situation is unlikely to change significantly.

---

238. CUSHMAN ET AL., *supra* note 237, at 8.

239. Below is a list of potential pitfalls:

- Employees may feel their privacy has been devalued or violated.
- It may be difficult to retain employees if monitoring seems intrusive.
- Monitoring can signal a lack of trust, which can breed resentment and reduce employee morale and productivity.
- The line between work and home may be blurred; people often use the same devices for both, so where does monitoring cross the line?
- Extra data means more information could be misused if it lands in the wrong hands.
- There are legal issues to contend with to ensure the employer remains within legal rights and respects employees’ rights. The more geographic areas the employer operates in, the more likely these regulations will differ in each area.
- Any monitoring program is only useful if it is actually scrutinized, which takes time and money.
- Surveillance may create a false sense of security, which can actually be a risk in and of itself.

Bridget Miller, *Pros and Cons of Employee Monitoring*, HR DAILY ADVISOR (Sept. 25, 2019), <https://hrdailyadvisor.blr.com/2019/09/25/pros-and-cons-of-employee-monitoring/> [https://perma.cc/7QYX-E4D4].

While remote operations make law firms more vulnerable to cyber-attacks, most law firms tend to disregard these risks unless their clients or regulators insist on the adoption of new cybersecurity measures. While a dramatic increase in successful cyber-attacks on law firms and other private-sector organizations might change this situation, profitability will remain the top objective of law firm partners. As a result, it is unlikely law firms will increase their investment in cybersecurity in the form of expensive equipment, software, services from outside contractors, and cyber-insurance policies with high face-values and expensive premiums. Perhaps law firms can find the needed funds by leasing less expensive office premises. A failure to find adequate funds for cybersecurity improvements will make law firms more vulnerable to cyber-attacks, but it also makes it difficult for them to comply with professional responsibility norms, thus resulting in greater legal malpractice and other risks.