fucile & reising | LLP

March 2021 WSBA *Bar News Ethics & the Law* Column

Don't Try This at Home: Responding to Cyber Intrusions and Data Breaches

By Mark J. Fucile
Fucile & Reising LLP

> "Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession."
> ~ABA Formal Opinion 483 at 1 (2018)

The Attorney General publishes an annual report on data breaches in Washington.[1] It makes sobering reading. The current report, its predecessors and related information on the Attorney General's web site collectively reflect that in recent years hundreds of businesses have had data breaches affecting thousands of Washington residents. Professional service firms are among the businesses reporting significant breaches.

When a data breach or other intrusion occurs at a law firm, panic is an understandable reaction. There may also be an all-too-human instinct to try to fix the problem without outside help. Even for larger firms—let alone small and mid-size ones—that runs the risk of compounding an already difficult situation. As they used to say on television when demonstrating something dangerous, "don't try this at home." Rather, a law firm will likely need help on two fronts. First, the firm should immediately retain technical assistance to determine the nature of the intrusion and whether information has been accessed, and to undertake any repairs or restoration necessary. Second, if personal information has been accessed, the firm will likely need legal help to navigate complex and overlapping

data breach notification laws. Even if personal information has not been accessed, the firm may still need legal help in notifying clients if, for example, the firm has been "locked out" of its files through a "ransomware" attack and time-sensitive ongoing matters will be affected while data is being restored. In this column, we'll survey both.

Before we do, however, three preliminary points are in order.

First, although we will focus here on aftereffects, firms must take reasonable proactive steps appropriate to their size and practice to guard against intrusions. Comment 8 to RPC 1.1 emphasizes that our duty of competence includes understanding the technology that we use in our practices. RPC 1.6(c), in turn, obliges us to "make reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[2] The leading ABA opinion on data breach response, quoted at the outset, notes that proactive steps include ongoing monitoring for potential intrusions, training firm lawyers and staff on security measures and response planning.[3] Advance planning should also include insurance. Malpractice policies may—or may not—include coverage for technical assistance in the wake of a breach and with any required notification. Firms, therefore,

should carefully review their coverage and obtain either a rider on their malpractice policy or a separate cyber risk policy.[4]

Second, many of the same considerations we will discuss for firm networks are triggered if an unencrypted firm laptop computer or other "smart device" is lost or stolen. In years past, a paper file left behind at a restaurant following lunch with a client would probably still be there when we returned to retrieve it. An expensive computer is both a more inviting target for thieves and for many lawyers may hold the functional equivalent of their entire "file room."[5]

Third, although a data breach or other intrusion is unquestionably bad, mishandling the response can make the situation immeasurably worse. In addition to any disciplinary consequences, the RPCs just noted are not too distant from the standard of care for legal malpractice.[6] The regulatory standards for protecting client confidentiality also broadly reflect our underlying fiduciary duty—raising the specter of further civil damage risk.[7] RCW 19.255.040 provides statutory remedies to both the Attorney General and consumers injured by reporting failures. Sophisticated clients who have incorporated their own reporting requirements into engagement agreements with law firms may also pursue breach of contract claims if the required reporting does not follow a

breach.[8] In short, firms face significant risk on a variety of fronts if they do not assess and handle intrusions appropriately.

Technical Help

Not all intrusions are created equal. Some may surreptitiously gain access to a law firm's network to steal sensitive client information. In one well-publicized incident, for example, hackers gained access to internal networks at several prominent New York law firms to read confidential emails discussing potential deals that had not yet been announced publicly so they could profit on the stock prices of the companies involved.[9] Others involving "ransomware" encrypt a firm's files and then demand money for the decryption key. Although some ransomware schemes involve accessing the files involved, others simply encrypt them.[10]

Once an intrusion is discovered, it is critical to get competent technical help in two primary areas without delay.

First, a forensic analysis should be undertaken to determine the nature of the intrusion and whether information has been accessed. If personal information of clients or others has been compromised, then the data breach notification laws discussed in the next section will likely have been triggered. By contrast, if the firm has simply been "locked out" of its files through a ransomware

attack, notification statutes may not have been triggered because no personal information has been accessed or taken. Even if notification statutes are not triggered, however, a firm still has a duty to inform clients under RPC 1.4—which addresses lawyer-client communication—if the firm's ability to continue clients' work is affected materially by its inability to access the files involved. ABA Formal Opinion 483 puts it this way:

> "[N]o notification is required if the lawyer's office file server was subject to a ransomware attack but no information relating to the representation of a client was inaccessible for any material amount of time, or was not accessed by or disclosed to unauthorized persons. Conversely, disclosure will be required if material client information was actually or reasonably suspected to have been accessed, disclosed or lost in a breach."[11]

If the firm has data breach insurance coverage, the carrier should be contacted immediately to coordinate the necessary technical assistance. If not, the firm's malpractice carrier will still be a valuable resource for referrals to the specialized forensic assistance needed.

Second, technical help will also likely be needed to stop the breach, repair the systems affected and restore any data lost.

Legal Help

If a breach has occurred and it is either apparent or reasonably likely that personal information has been compromised, RCW Chapter 19.255 outlines

disclosure obligations. RCW 19.255.005(1) and RCW 19.255.005(2) define, respectively, "breach" and "personal information." The former is framed as the "unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information" and the later includes identifying information such as Social Security numbers, driver's license numbers and dates of birth. RCW 19.255.010, in turn, addresses the timing, content, and means for notice in the event a breach that includes defined personal information. Although law firms instinctively think in terms of clients, notice in this context extends to both clients and non-clients affected.[12] A defense firm, for example, might have plaintiffs' medical or tax records in its electronic files. If the breach involves more than 500 Washington residents, the Attorney General must also be notified under RCW 19.255.010(7).

Depending on the information involved, RCW Chapter 19.255 may just be the starting point. For a firm with clients from multiple states impacted, analogous statutes in the other states enter the mix.[13] Although statutes in this area are generally similar, they are not uniform. The nuances of each jurisdiction involved, therefore, must be parsed. Further, depending on the type of information compromised, specialized federal statutes protecting medical or

financial privacy may also come into play.[14] Depending on the residence of the persons involved, foreign laws may be involved as well.[15]

Given this complexity, it is not surprising that cyber security has become a distinct practice area. In light of the complexity, the comparatively short deadlines for notification in the statutes involved, and the penalties for failure to meet the requirements, the immediate aftermath of a breach is not a good time to learn a new area of law. For firms with cyber insurance, the carrier should be contacted promptly so it can also arrange for appropriate legal help. For those without insurance, the firm's malpractice carrier remains a practical resource for referrals. Firms specializing in this area can also usually assist with associated facets ranging from interfacing with law enforcement to analyzing insurance coverage for business interruption and claims against the firm from the breach.

Summing Up

Law firms are in the information business. As a result, we are targets for bad actors who either want to steal that information or hold it hostage. In addition to proactive security, firms must also respond appropriately in the event of a breach or other intrusion. Given the technical and legal complexity involved, getting specialized help is critical. In short, "don't try this at home."

ABOUT THE AUTHOR

Mark J. Fucile of Fucile & Reising LLP handles professional responsibility, risk management and attorney-client privilege issues for lawyers, law firms and corporate and governmental legal departments throughout the Northwest. Mark has chaired both the WSBA Committee on Professional Ethics and its predecessor, the WSBA Rules of Professional Conduct Committee. Mark is a member of the Oregon State Bar Legal Ethics Committee and the Idaho State Bar Section on Professionalism & Ethics. Mark writes the Ethics Focus column for the Multnomah (Portland) Bar's *Multnomah Lawyer*, the Ethics & the Law column for the WSBA *Bar News* and is a regular contributor on legal ethics to the WSBA *NWSidebar* blog. Mark is a contributing author/editor for the current editions of the OSB *Ethical Oregon Lawyer*, the WSBA *Legal Ethics Deskbook* and the WSBA *Law of Lawyering in Washington*. Before co-founding Fucile & Reising LLP in 2005, Mark was a partner and in-house ethics counsel for a large Northwest regional firm. He also teaches legal ethics as an adjunct for the University of Oregon School of Law at its Portland campus. Mark is admitted in Oregon, Washington, Idaho, Alaska and the District of Columbia. He is a graduate of the UCLA School of Law. Mark's telephone and email are 503.224.4895 and Mark@frllp.com.

---

[1] The report and associated materials are available at: https://www.atg.wa.gov/data-breach-notifications. The ABA also publishes a Legal Technology Survey Report annually that includes cybersecurity information specific to law practice. It is available on the ABA web site.

[2] *See generally* WSBA Advisory Ops. 2215 (2012) (cloud computing) and 201601 (2016) (virtual offices).

[3] *See also* ABA Formal Op. 482 (2018) (disaster planning generally); ABA Formal Ops. 477R (2017) (data storage and transmission security) and 99-413 (1999) (email security).

[4] *See generally* Jill D. Rhodes and Robert S. Litt, *The ABA Cybersecurity Handbook*, ch.15 (2d ed. 2018) (an excellent resource with the referenced chapter focusing on insurance).

[5] *See generally* Cal. Interim Eth. Op. 16-0002 (2019) (analyzing scenarios involving lost and stolen law firm laptops and mobile phones).

[6] *See* WPI 107.04 (standard of care for legal malpractice).

[7] *See generally Eriks v. Denver*, 118 Wn.2d 451, 824 P.2d 1207 (1992) (discussing relationship between professional rules and fiduciary duties); *see, e.g., Wengui v. Clark Hill, PLC*, 440 F. Supp.3d 30 (D.D.C. 2020) (discussing law firm liability for legal malpractice and breach of fiduciary duty to client for cyber intrusion exposing client's personal information).

[8] *See, e.g., Hiscox Insurance Company, Inc. v. Warden Grier, LLP*, No. 4:20-cv-00237-NKL (W.D. Mo.) (complaint filed March 27, 2020) (alleging that law firm breached contractual terms of engagement by failing to notify plaintiff of data breach).

[9] *See* Leslie Picker, "3 Men Made Millions by Hacking Merger Lawyers, U.S. Says," *The New York Times*, Dec. 27, 2016.

[10] *See generally* Nathaniel Popper, "Ransomware Attacks Grow, Crippling Cities and Businesses," *The New York Times*, Feb. 9, 2020.

[11] *Id*. at 14.

[12] ABA Formal Opinion 483 notes as to clients (at 10-15) that although Model Rule 1.4 is only framed in terms of current clients, data breach statutes generally extend reporting obligations to former clients as well.

[13] *See, e.g.*, Alaska Stat. § 45.48.010; Idaho Code § 28-51-105; Or. Rev. Stat. § 646A.604; *see generally ABA Cybersecurity Handbook*, *supra*, Apps. B (state reporting statutes) and D (state regulations).

[14] *See generally ABA Cybersecurity Handboo*k, *supra*, Apps. A (federal reporting statutes) and C (federal regulations).

[15] *See, e.g.,* European Union General Data Protection Regulation, available at www.gdpr.eu; *see generally ABA Cybersecurity Handbook*, *supra*, ch. 5 (addressing international aspects).