Cybersecurity Threats to Law Firms:

Risk and Mitigation

by Jeromy Simonovic and Robert (Bob) L. Kardell

Background

The tenuous outlook on the state of cybersecurity around the globe is shaped by an unsettling reality where any business or individual will be targeted for cyber criminals to exploit.[1] As the use of internet and technology becomes even more ingrained into every facet of our lives, so increases the complexities of electronically storing data and our vulnerability to hacking, ransom demands, and other cyber-crimes. While cybersecurity concerns pre-date the chaotic environment brought on by COVID-19, pandemic induced shutdowns amplified existing security vulnerabilities for many businesses operating remotely, emboldening cyber criminals to unleash a torrent of internet crimes that has yet to be contained. The FBI reported that it received a record number of internet crime complaints in 2020, representing a 69% overall increase from 2019.[2] Cybercriminals have shown to be equal opportunity offenders lodging attacks against all sectors including an exponential increase against healthcare, manufacturing, and finance in 2020.[3] This uncertain time also exacerbated a disturbing trend with law firms as prime targets for cybercriminals during a precarious period when many firms shifted to virtual operations despite lacking sufficient infrastructure.[4] When the heightened risk of incurring a cyber-attack coincides with the increasing use of technology, attorneys must remain keenly aware of several ongoing responsibilities, including professional obligations to prevent security incidents.[5]

Threats to Law Firms and Directed Attacks

Cybersecurity risks in the legal profession are certainly not a new development. It has been estimated that at least 80 of the 100 largest law firms have had "some sort of breach" over the last few years.[6] It should come as no surprise that law firms are attractive targets for cybercriminals seeking to steal, expose, sell, or otherwise extort valuable and confidential information. Despite the heightened focus on cybersecurity, incidents such

Jeromy Simonovic

Jeromy Simonovic is an Ohio licensed attorney and serves as General Counsel at Digital Forensics Corp. He has significant experience and knowledge within the areas of computer forensics, electronic evidence, cybersecurity, and data privacy. As an adjunct professor teaching cyberlaw and advanced legal technology, Jeromy continually follows the rapid developments in cybersecurity as well as emerging technologies that impact and improve the legal industry. For more information, Jeromy can be contacted at (216) 255-6269 or Jeromy.S@digitalforensics.com.

Robert L. Kardell

Robert L. (Bob) Kardell is a Nebraska licensed attorney at Baird Holm, LLP, whose practice focuses on cyber-breach incident response, legal and technology-based risk management solutions, technology and cyber-defense policy and protections, intrusion remediation, and fraud prevention and investigation. Bob has more than twenty-two (22) years of experience working for the Federal Bureau of Investigation as a Special Agent and Supervisory Special Agent. Bob was an expert computer forensics examiner and a financial forensics examiner during his career before engaging in the practice of law.

as ransomware attacks, social engineering campaigns, business email compromise, and other cybercrimes remain a significant threat for law firms.

Law firms are prime targets for many reasons. Hackers know the type of data a law firm retains is valuable. The data can include financial statements, tax information of corporations and individuals, information on mergers and acquisitions, trial strategy, sensitive divorce information, and more. In fact, the larger the firm the more likely the firm has extensive sensitive information, which could be valuable to the hackers or on the dark web.

The threats to law firms stem from several vulnerabilities rooted in how law firms operate. Law firms generally suffer from a lack of strong internal controls and compliance programs leaving law firms open to cyber-attacks. Law firms also engage in discovery, whereby they are required to accept digital files or share a common repository of digital data as part of the discovery process, litigation, client engagement, investigations, due diligence, and more. Most law firms communicate primarily by email, which also makes the firms vulnerable to phishing and malware propagated via email. All these processes require law firms to accept and engage in activities which put their networks at risk.

Besides external threat actors, law firms may also encounter various cybersecurity risks from personnel within the firm.[7] Considering this massive exposure, it is not evident that the legal industry is handling data security in a manner commensurate to grasping the severity of the issues. According to the American Bar Association's 2020 survey of technology use among law firms, only a minority of law firms employ widely recommended data security technologies and practices.[8] Attorneys that suffer a security incident must be also aware of several sources obligating them to take certain action when a data breach or security intrusion has occurred.

Professional Obligations

Like all businesses, attorneys must too be vigilant in the aftermath of a security incident, but, perhaps more importantly, attorneys must also take reasonable precautions to avoid incidents occurring in the first place. The failure to employ safeguards could lead to severe repercussions, including federal investigations, malpractice suits, ethical violations, fines, and irreparable reputational harm. Attorneys are precluded from pleading ignorance of new technologies, particularly as it concerns protecting client data. In 2012, the American Bar Association updated its model rules to require lawyers to stay abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology. The duty of competence meant that in addition to substantive knowledge of the law, lawyers are required to practice the competent use of technology used to practice law. The model rules do not require lawyers to be technology experts, but all lawyers are required to have at least a basic understanding of the technologies they and their clients use.

Several of the ABA Model Rules have application to the protection of client information, including competence (Model Rule 1.1), communication (Model Rule 1.4), the confidentiality of information (Model Rule 1.6), safeguarding property (Model Rule 1.15), and supervision (Model Rules 5.1, 5.2, and 5.3).

The 2012 amendments include addition of the following underlined language to the Comment to Model Rule 1.1:

> "[8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, <u>including the benefits and risks associated with relevant technology</u>..."

The ethics rules require attorneys to take competent and reasonable measures to safeguard information relating to clients (ABA Model Rules 1.1 and 1.6 and Comments). Compliance requires attorneys to understand limitations in their knowledge and obtain sufficient information to protect client information, to get qualified assistance if necessary, or both. These obligations are minimum standards—failure to comply with them may constitute unethical or unlawful conduct. Attorneys should aim for security that goes beyond these minimums as a matter of sound professional practice and client service.

Model Rule 1.4 requires attorneys to make sure that clients are "reasonably informed about the status of the matter" and to "explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."

Further, Model Rule 1.6 states that lawyers must make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Comment 8 to Model Rule 1 explains that, in order to maintain the required knowledge and skill, lawyers should stay abreast of all changes "including the benefits and risks associated with relevant technology."

ABA Formal Opinion 483

The American Bar Association provided guidance in "Lawyers' Obligations after an Electronic Data Breach or Cyberattack (ABA Formal Opinion 483, October 17, 2018)." The Opinion provides that lawyers have a duty to make "reasonable efforts to avoid data loss or to detect cyber-intrusion," and that an ethical violation may occur if the lawyer does not undertake these steps. As a response, many law firms have adopted cybersecurity obligations to protect their clients' data and the firm's integrity and reputation.[9]

Opinion 483 defines a data breach as an intrusion that results in the loss of "material client information," or one that "significantly impair[s]" the attorney's ability to provide legal

services. However, the qualifiers "material" and "significantly" suggest that not all data breaches trigger a duty to notify clients. The opinion further provides that "the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach." The opinion also states that "as a matter of preparation and best practices...lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach."

This opinion is significant in that it imposes a duty to provide breach notifications to clients if "material client information was actually or reasonably suspected to have been accessed, disclosed or lost in a breach."[10] This duty is greater than most, if not all, of the state breach notification laws. Most state breach notification laws require notification if the data is acquired or accessed, and do impose a notification requirement if the data is not actually acquired or accessed. The ABA, on the other hand, imposes a requirement or a duty of notification if the client information was *reasonably suspected to have been accessed.* This is a much lower threshold.

Thus, while a breach may not be reportable under state law, a lawyer or a law firm may nonetheless have a duty or an obligation to provide notification to affected individuals according to this ABA Opinion.

ABA Formal Opinion 498 – Considerations Involving Virtual Practice of Law

Like most businesses, COVID-19 necessitated drastic changes to most aspects of the legal profession, with court hearings and highly sensitive discussions being held via video-conference. Virtual practice began years ago but has accelerated because of enhanced technology usage by both clients and lawyers and increased need. Although the ethics rules apply to both traditional and virtual law practice, virtual practice was the subject of ABA Formal Opinion 498.

On March 10, 2021, the Standing Committee on Ethics and Professional Responsibility of the ABA released Formal Opinion 498. In that opinion, the ABA recognizes the need for the virtual practice of law but emphasizes the responsibilities attorneys face when engaged in the practice. The opinion emphasizes that attorneys should read and understand all of the terms of service for any platform used to engage in client engagements. Attorneys should understand how the platform will use the information collected and what type of encryption is used. Security considerations may include whether there are differences between free, personal, or commercial platforms and to use the most appropriate forum to ensure the confidentiality of client data. The opinion states:

> *Lawyers should be diligent in installing any security-related updates and using strong passwords, antivirus software, and encryption. When connecting over Wi-Fi, lawyers should ensure that the routers are secure and should consider using virtual private networks (VPNs).*

Thus, the duty to protect client data is an ongoing duty that does not end when the correct platform and security options are selected. The duty continues throughout the use of the platform and, more generally, technology. The duty requires ongoing updates and security implementation for software and hardware. The duty requires an understanding as to the security regarding the encryption technology used, the security of the storage technology, and an understanding as to password strength and how multifactor authentication can affect client security.

This same level of understanding is imposed on attorneys regardless of the platform, and applies to video conferencing, sharing client files, accessing client files or resources, smart speakers, audio conferencing, and all other technology platforms.

State Notifications

In addition to ethical obligations of the profession, lawyers and firms are bound to any applicable state laws governing information security and data breach obligations. Legislative attention in this area is rampant as evidenced by the Stop Hacks and Improve Electronic Data Security ("SHIELD") Act enacted by New York in 2019 and the California Consumer Privacy Act ("CCPA"), which became effective in January 2020. As with any business, the applicable data breach notification statutes must be carefully examined to determine if the breach has caused the exposure of data protected by the statute, and in a sufficient amount to trigger a duty to notify. In some states, small-scale data breaches will not trigger a notification obligation. In others, notice of any breach must be provided to the affected party or the state attorney general, or both.

Every state, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches that involve personal information, and, depending on the types of information involved in the breach, other laws or regulations may impose additional obligations. In many circumstances, companies are under strict timelines to notify impacted individuals and report the breach to the authorities, credit-reporting agencies, and more. Since the CCPA was passed in 2018, multiple states have proposed consumer protection laws. On March 2, 2021, Virginia became the second U.S. state to enact a comprehensive data privacy law. Colorado became the third state to enact such a law with the Colorado Privacy Act on July 7, 2021.

Regulations - Contractual and Federal Obligations

Companies must also be prepared to comply with the legal obligations to individuals, state attorney generals, and other regulatory bodies in the aftermath of a breach. Attorneys have common law duties to protect client information, and often have contractual and regulatory obligations to protect information relating to clients and other personally identifiable information. While there is no federal law regulating a law firm's cybersecurity practices and policies, the federal law does regulate specific industry practices. For instance, if a law firm has a client within the healthcare, accounting, or financial industry sectors, additional federal obligations may apply. Clients in the financial industry sector may require that their law firms maintain extra security protection due to the sensitive nature of financial data. The same applies for healthcare companies

who store confidential health records of the public. Clients that specialize in accounting practices must comply with the Sarbanes–Oxley Act of 2002, which could impose additional obligations on the law firms representing those clients.

Encryption as a Security Method – Formal Opinion 477

During the last several years, some state ethics opinions have increasingly expressed the view that encryption of email may sometimes be required to comply with attorneys' duty of confidentiality. On May 11, 2021, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477, "Securing Communication of Protected Client Information." The opinion revisits attorneys' duty to use encryption and other safeguards to protect email and electronic communications in light of evolving threats, developing technology, and available safeguards. It suggests a fact-based analysis and concludes "the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication," but "particularly strong protective measures, like encryption, are warranted in some circumstances." It notes that attorneys are required to use special security precautions, like encryption, "when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security."

The ABA Standing Committee on Ethics and Professional Responsibility Opinion 477R (Revised May 22, 2017) imposes a fact-specific obligation on lawyers to undertake "reasonable efforts to prevent inadvertent or unauthorized access" to client information arising from cyberattacks. The reasonable efforts standard:

> Rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligation 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.[11]

The opinion also provides a list of factors to consider when determining the severity of the preventative measures that must be implemented in order to fulfill this obligation, including the:

- Sensitivity of the information;
- Likelihood of inadvertent disclosure;
- Cost and difficulty of implementing safeguards; and
- Extent to which the safeguard will impede the lawyer's ability to represent their client.

Proactive Steps for Protection

Law firms can take several proactive steps to protect their client's data and to protect themselves from liability.

Use of Encryption

As stated above, encryption has become almost as common as computers themselves. In fact, most of the devices we carry are encrypted by default, including phones, tablets, and laptop computers. What was an expensive and sometimes cumbersome software years ago is now built seamlessly into the modern devices. Microsoft Windows comes with BitLocker, a whole disk encryption system, built directly into the system. Encryption is enabled by default in most business computers and laptops. Several of the file system encryption programs can also be used on USB devices to provide encryption on removable devices.

Encryption on the internet is now commonplace as well. In just a few years, the internet has moved from unencrypted uniform resource locators ("URL") starting with "http" to now "https." The "s" at the end of "https" stands for "secure" through the use of encrypted traffic. Traffic traversing over the secure connection uses Transport Layer Security ("TLS"), operates on a different port than http traffic (port 443 rather than port 80), and creates a secure connection between the

web browser and the web site before transferring information between the two. TSL protects the information from packet sniffing tools such as Wireshark and other hacking tools.

Finally, email traffic can be encrypted as well. Email clients such as Outlook and web clients such as Gmail, Yahoo!, or Outlook.com, can be configured to send mail encrypted if possible. Such encryption is possible without the user knowing the encryption keys because the whole process will occur automatically behind the application. If needed, however, email servers can be configured to connect directly to an established server via an encrypted connection.

Many state laws have exemptions for the loss of encrypted systems. If encrypted, a lost laptop or USB drive would no longer be a reportable event. It would meet the standards of the ABA rules of preventing a reasonable likelihood of a hacker or other being able to read the data.

Multifactor Authentication

Multifactor authentication ("MFA") requires a user to provide alternative forms of proof before allowing the user access to the system. The alternative proof can be something the user has, such as a key fob or an authenticator application on their phone; the proof can be something the user is, such as a fingerprint, a retina scanner, or a facial scan currently used by the iPhone or Windows "Hello;" or the additional proof may be somewhere the user is, such as the IP address at work or at home or a geographic location. Whatever that additional security factor may be, employing MFA may be the single biggest deterrent someone could employ.

There are many studies which suggest that phishing schemes, which attempt to trick users into divulging credentials and compromised credentials, may be the single most used method for hackers to attack and breach networks. By some estimates, this type of attack accounts for 75% to 90% of all attacks.

Firewall Software or Hardware Devices

In addition to software protections, lawyers and law firms should invest in proactive protections such as software or hardware firewalls. A firewall can be configured to protect your system from scans, DOS/D-DOS attacks, and many other attacks. Firewalls also commonly log traffic passing through the firewall from the internal traffic to the Internet, and from the Internet to the internal network. The logs kept by the firewall can be very useful when attempting to recover from a true hacking attack. The logs, if configured correctly, can help determine if exfiltration has taken place, if hacking tools were downloaded, and the IP address of the attacker.

Firewalls which are maintained on a separate hardware device or separate from an internal domain may survive a hacking attack. The evidence maintained on and collected by the firewall may be the evidence necessary to make a determination as to whether notification will be necessary to clients and others whose information is on the internal network.

Virtual Private Networks

Virtual Private Networks ("VPN") can be established by a hardware device, sometimes run on a firewall, or can be provided by a software platform. VPNs can provide protections to an internal network while enabling that internal network to connect to another network seamlessly while maintaining the privacy of that connection and the files being shared through that connection.

VPNs can also provide protection to the internal network by hiding the IP address of the network. If a computer uses a VPN, its IP address will appear to be the IP address of that server. This can have several benefits including hiding the internal network IP address, hiding the location of the IP server, and providing that secure data transfer.

Protect Mobile Devices

Protecting mobile devices is just as important as protecting computers, servers, laptops, desktops, etc. There are more mobile devices being used to connect to services and systems than laptops and desktops. Many people of have multiple mobile devices such as multiple phones and tablets, but yet many only have a single desktop or laptop.

Keeping all Devices Up to Date

One of the biggest, if not the biggest, vulnerability issue is not patching systems and computers in a timely manner. New exploits to computer operating systems, applications, mobile devices, and IOT devices are announced every day. As these exploits are announced, hackers will attempt to search and find for vulnerable systems and exploit the systems before the patches or updates can be installed and applied. Keeping devices up to date is not always easy and keeping a network of devices up to date can be difficult and complex, but making a regular schedule to ensure updates and patches are applied should be part of every organization's cybersecurity plan.

Conclusion

Law firms are targets of cyber hackers due to the type and volume of personal data that is kept on their systems. Lawyers have many obligations from ethics rules to legal and regulatory requirements to protect client's data entrusted to them. There are numerous methods available to protect networks, mobile devices, computers, and client data. Lawyers should us the utmost care to secure their clients' data to ensure the security of the data. Failure to do so may result in a data breach and notifications to clients, as well as possible fines and a regulatory investigation.

Endnotes

1 *Cybersecurity recognizes a world where law enforcement discusses hacking and data loss in terms of "when," and not "if."* ABA Formal Opinion 477, Securing Communication of Protected Client Information (May 11, 2017).

2 2020 Internet Crime Report, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

3 Healthcare, manufacturing, and finance industries targeted 200%, 300% and 53% respectively form year prior 2021 Global Threat Intelligence Report (GTIR) released by NTT, https://hello.global.ntt/en-us/insights/2021-global-threat-intelligence-report/.

4 Zack Needles, Trendspotter: *Law Firms Keep Getting Cyberscammed—and COVID-19 Isn't Helping*, Law.com (Aug. 2, 2020), https://www.law.com/2020/08/02/law-com-trendspotter-law-firms-keep-getting-cyberscammed-and-covid-19-isnt-helping.

5 Various states version of Duty of Technology Competence, https://www.lawsitesblog.com/tech-competence.

6 Ellen Rosen, *Most Big Firms Have Had Some Hacking: Business of Law*, Bloomberg (Mar. 11, 2015), https://www.bloomberg.com/news/articles/2015-03-11/most-big-firms-have-had-some-form-of-hacking-business-of-law?sref=OOpRUZ8l.

7 Dr. Nick Oberheiden, *5 Cybersecurity Risks and 3 Obligations for Law Firms*, The National Law Review, https://www.natlawreview.com/article/5-cybersecurity-risks-and-3-obligations-law-firms.

8 John G. Loughnane, 2020 Cybersecurity, American Bar Association, https://www.americanbar.org/groups/law_practice/publications/techreport/2020/cybersecurity/.

9 Dr. Nick Oberheiden, *5 Cybersecurity Risks and 3 Obligations for Law Firms*, The National Law Review, https://www.natlawreview.com/article/5-cybersecurity-risks-and-3-obligations-law-firms.

10 ABA Formal Opinion 483 at p. 14.

11 *See* Opinion 477R (Revised May 22, 2017).