INFORMATION PRIVACY AND CYBERSECURITY RESPONSIBILITIES, LIABILITIES, STRATEGIES, AND TACTICS

JEFFREY B. MILLER of the Lancaster office of Saxton & Stump is a transactional, commercial, regulatory, and compliance attorney for clients involved in healthcare and the life sciences, as well as other areas of business. He is a member of the firm's Corporate Healthcare and Life Sciences, Mergers and Acquisitions, Risk Mitigation and Safety, and Investigations and Criminal Defense groups. Jeff also provides support to the firm's Commercial Litigation team. In addition to his legal work, Jeff is Director-in-Charge of Granite Governance, Risk and Compliance, an affiliated international consulting firm that helps leaders solve their business' most complex and critical challenges, including challenges involving information privacy and security.

ANTHONY SIMS is a Cyber Security Analyst at Granite Governance, Risk and Compliance, LLC. As a former Cyber Attacker for the US Navy, Anthony performed enterprise cybersecurity management, network defense, risk assessment, security governance, and technology implementation. He also participated in the NSA-certified Joint Cyber Analysis course, focused on programming, OS architecture, network analysis, and malware analysis.

The authors can be reached at jbm@saxtonstump.com or at jbm@granitegrcconsulting.com.

"Three may keep a secret, if two of them are dead."

- Benjamin Franklin, Poor Richard's Almanac

From law firms with fewer than 10 attorneys to those with more than 500 and from bar associations to state courthouses, dozens of organizations involved in the legal profession have reported experiencing cyberattacks compromising their confidential information in the past few years. The American Bar Association (ABA) reported that more than 100 such organizations disclosed similar attacks from 2014 to 2019; and more than one in four law firms disclosed experiencing data breaches from 2021 to 2022. In the first quarter of 2023, the global rate of cyberattacks rose by seven percent, with one in 40 focused on law firms or insurance providers, proving it to be an accelerating (albeit not new) phenomenon.

Not surprisingly, attorneys regardless of firm size have voiced significant and increasing concerns over protecting the privacy and security of the confidential information entrusted to them. When it comes to security defenses, however, many law firms lag well behind most other organizations, including their own clients. According to the ABA report, only 49 percent of firms regularly use file encryption and only 40 percent regularly use email encryption—both common cybersecurity defense techniques used by businesses across the country.

The result is that hackers have come to view the legal profession as a preferred point of attack. Data breaches at five prominent law firms made the news in 2023. These incidents are not just a mess that firms must clean up in house. Clients-become-plaintiffs have filed at least five class actions claiming that the named firms failed in their duties to sufficiently guard confidential information against disclosure.

In response to these pressures, many firms have wisely added cyber insurance policies to their insurance portfolios. Unfortunately, while helpful, even the best cyber insurance policies do not come close

to adequately mitigating the damages caused by data breaches. Attorneys and their firms cannot insure against the time lost in opening locked-down systems and retrieving lost data. Nor can they insure against the licensure implications of failing to comply with professional ethical rules that require better safeguards or the potentially serious penalties associated with violations of federal and state laws. There are also important questions involving the waiver of attorney-client privilege where attorneys fail to take reasonable measures to safeguard the confidentiality of their clients' information. Consider also the significant costs of losing clients and the negative public relations implications of losing control of sensitive and confidential client information—information that is often sold to the highest bidder on the dark web or made public. The limitations of cyber insurance could not be any clearer, making it especially important that attorneys proactively manage and mitigate cyber risks both before and in response to attacks when they occur.

ABA MODEL RULES OF PROFESSIONAL CONDUCT

A variety of attorney ethical rules clearly require attorneys to take objectively reasonable measures to identify and manage these risks. Our analysis focuses on the ABA Model Rules of Professional Conduct.

The ABA Model Rules of Professional Conduct make it clear that attorneys shoulder the obligation to maintain the confidentiality of their clients' information in whatever technological environment they work within. ABA Model Rule Section 1.1 provides that "[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[1] Focusing on the technological environment, Comment 8 to Model Rule 1 makes clear that "[t]o 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." Clearly in today's day and age, under the ABA Model Rules, the duty of competency requires a reasonable level cybersecurity understanding.

The ABA Model Rules also make it clear that attorneys have an obligation to ensure that the tools used to maintain and communicate client information are secure. ABA Model Rule Section 1.6(c) provides that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Comment 18 sets forth the factors to be considered in determining the reasonableness of the lawyer's efforts, including, but not limited to:

> the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[2]

ABA Formal Opinion 477 adds additional clarity, providing that:

> [a] lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.[3]

Following upon Formal Opinion 477, Formal Opinion 483 strikes directly at the matter of cybersecurity, stating "[t]he 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."[4] Opinion 483 further states that "[a]s 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."[5]

In a world where most information is received, stored, used, and transmitted electronically, the ABA Model Rules require attorneys to undertake proactive reasonable efforts to protect that information, and to prepare to respond to potential breaches.

FEDERAL AND STATE LAWS

In addition to attorney ethical rules, multiple federal laws governing the protection of certain information require attorneys and their firms to take proactive, effective actions to safeguard that information. While a full accounting and explanation of the federal laws are beyond the scope of this article, many law firms face one central and well-known law—the Health Insurance Portability and Accountability Act of 1996, and its progeny law, the Health Information Technology for Economic and Clinical Health Act (together as HIPAA).[6] As HIPAA business associates, law firms that receive, store, use, or transmit HIPAA-defined Protected Health Information are required to maintain adherence to HIPAA's privacy and security requirements.

For information security, HIPAA provides the HIPAA Security Rule, containing more than 60 required or addressable actions. Serious civil and/or criminal penalties can be assessed for violations of HIPAA's requirements. For the years 2023 and 2024, civil penalties range between $137 per violation to a whopping $68,928 per violation, depending upon level of culpability, with an annual penalty limit of $2,067,813. Criminal penalties can include fines of up to $250,000, imprisonment of up to 10 years, or both.[7]

In addition to the federal laws, numerous states have enacted laws that require businesses that own, license, or maintain personal information to implement and maintain "reasonable security procedures and practices" to protect personal information from unauthorized access.[8] At this time, all 50 states and the District of Columbia have enacted legislation requiring businesses and other entities to notify affected individuals when data breaches involving their personal information occur.[9] In addition, 32 states plus the District of Columbia require that notice of the breaches be made to certain state agencies and law enforcement authorities, typically to the state attorney general's office and/or office of consumer protection.[10]

CYBERSECURITY STRATEGIES FOR YOUR FIRM

Industry-specific guidelines offer a roadmap for enhancing cybersecurity posture for law firms and other organizations alike. These guidelines cover a spectrum of recommendations, from implementing robust access controls and encryption protocols to providing regular security training. Adhering to these guidelines not only helps in meeting regulatory requirements but also demonstrates a commitment to client confidentiality and security. Implementing and adhering to these industry standards helps organizations build a strong foundation for their information privacy and security programs at the operational level.

There are many accepted professional and technical standards that can be used to assess and improve cybersecurity at law firms. Two of the most commonly utilized standards are:

- ISO/IEC 27001: Commonly referred to as ISO 27001, this is an international standard for information security management systems.[11] ISO 27001 provides a set of controls that are applicable to organizations of all types and sizes and that are designed to preserve the confidentiality, integrity, and availability of information by applying comprehensive and strategic risk management processes.
- NIST Cybersecurity Framework: The National Institute of Standards and Technology (NIST) provides a structured approach for assessing and improving cybersecurity risk management.[12] Adaptable for organizations of all types and sizes, the NIST guidelines provide detailed but highly customizable processes that organizations can use to prioritize the activities that are important most critical and apply their resources to maximize cybersecurity impact.

It is notable that HIPAA provides its own requirements related to information privacy and security and, in doing so, refers to and provides a crosswalk to the NIST Cybersecurity Framework, recommending application of the NIST standards for ensuring compliance with the HIPAA Security Rule.

A robust information privacy and security program at the operational level is vital for safeguarding sensitive data within any organization. Typically spearheaded by a chief information privacy and security officer or a similar executive role, these programs establish the use of a recognized cybersecurity standard, build controls around that standard and measure effectiveness against that standard though structured risk assessments and gap remediation. The HIPAA Security Rule requires law firms subject to HIPAA to perform such risk assessments and remediation any gaps annually.

Information privacy and security programs, including gaps remediation, do not occur on their own. Maintaining a system of controls to prevent security lapses and to identify and properly resolve those lapses when they occur is key to an effective program. Appropriate controls can vary depending on the firm and its circumstances. Basic controls involving the right policies and procedures, training programs, and defined lines of communication support the firm's ability to effectively secure its confidential information. Policies and procedures clarify the firm's required approach to its risks, while education and training programs instruct colleagues on the firm's security practices and enhance their understanding of evolving threats. Frequent training for colleagues focusing on the "dos and don'ts" of cybersecurity can help to prevent a considerable number of data breaches. Ensuring clearly defined lines of communication between colleagues and security management also helps to minimize security lapses and ensure that any lapses are resolved as quickly and efficiently as possible.

In addition to these basic controls, there are a number of technical controls that firms should consider to protect their confidential information.

Access Control Measures

These measures provide a least-privileged approach that only provides data access to the individuals who require it, supported by continuous monitoring and regular security audits to detect and respond to potential vulnerabilities.

Password Policies

Proper password policies vary based on business needs and the cyber standards applied. That said, they generally require the creation of complex passwords using a combination of letters, numbers, and symbols that are a minimum of 12 characters and contain upper- and lowercase letters. Among other points, NIST provides that passwords should be long and complex and never used for more than one system. Forced password changes should only occur where there is an indication of a breach.

Data Encryption

Ensuring the security of confidential information is paramount, and robust data encryption practices play a pivotal role in safeguarding this data. Law firms should encrypt confidential information both in transit and at rest. As part of these controls, firms should establish stringent rules for email use that mitigate against phishing attacks and malware distribution.

Network Segmentation

Implementing proper network segmentation through a zero-trust framework is a strategic approach to security that operates on the assumption that the network is already compromised. This methodology involves effectively partitioning network resources to impede lateral movement by potential attackers. By adopting a zero-trust model, security controls are dispersed throughout the network, creating barriers that significantly hinder unauthorized access. Properly segmenting a network in anticipation of a breach is crucial in minimizing the potential damage caused by attackers. Through this approach, the impact of a security incident is not only mitigated but also localized,

preventing the lateral spread of threats. The value of such segmentation lies in its ability to fortify the network against potential breaches, ensuring that even if one segment is compromised, the rest of the network remains resilient and secure.

Continuous Monitoring

Security tools that continuously monitor network activities and that ensure the timely application of software updates and patches are critical to intercepting, quarantining, and resolving cyberattacks. Not only does this software aid in incident detection and resolution, but it also supports forensic analysis and provides valuable audit trails for compliance purposes.

Incident Response/Disaster Recovery Plan

Even with the very best security protection available, law firms and other organizations still remain at risk of a data breach. As a result, it is essential (and required by HIPAA and the other standards described above) to prepare for that inevitability by having a formal incident response/disaster recovery plan. This plan should address procedures for preparation, data backups and availability, incident detection and analysis, containment, eradication, recovery, and post-incident assessment, as well as communication to reporting entities, government agencies, and clients.

FINAL ANALYSIS

Cybersecurity underinvestment can cause real financial harm to law firms in ways that make it more affordable to have an information security management system in place to protect sensitive client information. For small- to medium-sized firms, the initial investment in a cybersecurity program handled internally can range from $15,000 to more than $65,000, depending on the products and services required and the size of the firm. While this initial investment can seem daunting, the costs of not implementing these programs can be highly damaging and even fatal.

The prevailing philosophy holds that a data breach is a question of when, not if. The legal industry stands at a point where the integration of robust cybersecurity measures transcends mere best practices; it emerges as a critical necessity. The consequences of a cybersecurity breach extend far beyond financial losses, reaching into the realm of irreparable damage to a firm's reputation and client trust. By staying informed about the evolving threat landscape, understanding legal obligations, and adopting proactive cybersecurity measures, law firms can fortify their defenses. In doing so, they not only protect their clients and themselves from potential devastation but also uphold the integrity of their esteemed profession in the digital age.

Notes

1 Model Rules of Pro. Conduct r. 1.1 (Am. Bar Ass'n 2024), available at https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/.

2 Id. at cmt. 18.

3 ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R (2017), available at https://www.americanbar.org/news/abanews/publications/youraba/2017/june-2017/aba-formal-opinion-477r--securing-communication-of-protected-cli/.

4 ABA Comm. on Pro. Ethics & Pro. Resp., Formal Op. 483 (2018), available at https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-op-483.pdf.

5 Id.

6 42 U.S.C. § 1320d; 42 U.S.C. §§ 300jj et seq.; §§1 7901 et seq.

7 45 C.F.R. part 102.

8 See Data Security Laws, Private Sector, National Conference of State Legislatures (May 29, 2019), available at https://www.ncsl.org/technology-and-communication/data-security-laws-private-sector.

9 Fed Trade Comm'n, Data Breach Response: A Guide for Business (2021), available at https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business.

10 Data Security Laws, supra note 8.

11 Int'l Org. for Standardization, Information security, cybersecurity and privacy protection — Information security management systems — Requirements (2022).

12 Nat'l Inst. of Standards and Tech., The NIST Cybersecurity Framework (CSF) 2.0 (2024), available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.