The Legal Intelligencer

Cybersecurity Strategies and Tactics for Pennsylvania Law Firms

If your law firm hasn't taken the proper steps to secure its confidential information, both its own and the private information of its clients, then consider the following reasons as to why steps should be promptly taken to improve security immediately.

By **Jeffrey B. Miller** | July 04, 2022

Jeffrey B. Miller, senior counselor with Saxton & Stump. Courtesy photo

Many cyberattacks are increasingly simple for bad actors to launch. At the same time, larger organizations are steadily becoming more difficult to infiltrate, forcing hackers to target smaller organizations that often have less sophisticated defenses. Over the past several years, these two trends have combined to put organizations with high-value data on notice, no matter their size. Hospitals, retailers, municipalities, government entities, even credit bureaus have all taken their turns dealing with significant data breaches. Now, law firms, with their highly confidential records, are being regularly targeted.

Since 2020 organizations across the legal profession, from law firms with less than a half-dozen attorneys to firms with more than 500, from city bar associations to state courthouses, have reported cyberattacks compromising their confidential information. At the same time reports continue to show law firms continue to be slow to protect themselves to cyberattacks compared to businesses in other industries. State and federal regulations, as well as basic attorney ethics standards, require that law firms be faster in adopting technology to thwart cyberattacks.

If your law firm hasn't taken the proper steps to secure its confidential information, both its own and the private information of its clients, then consider the following reasons as to why steps should be promptly taken to improve security immediately.

Attorney Ethical Rules

There are a variety of ethical rules that clearly govern attorneys' obligations to take reasonable measures to maintain the confidentiality of their clients' information. These rules are described in both national model rules, as well as state-level attorney codes of professional ethics.

The American Bar Association 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. Focusing on the technological environment, Comment 8 to Model Rule 1 states: "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." Similar to the ABA Model Rules, Pennsylvania's 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 in. Focusing on the technological environment, Comment 8 to Pennsylvania Rule 1 states that: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject." Another piece of the rule states, "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." Because communication today is so often conducted by electronic means, it is clear that attorneys have an obligation to ensure that the tools used to communicate are secure.

While the Pennsylvania rules may not spell out a requirement that cyber security precautions be taken, the similarity between the Pennsylvania rules and the ABA Model Rules tend toward an interpretation that these precautions may be required.

Data Security Laws

- **Federal Laws**

In addition to attorney ethical rules, data security laws governing the protection of certain information also require attorneys to take proactive, effective actions to protect that information. The failure to do so can result in significant fines and penalties.

For laws firms working in the health care area, one central and well-known federal law is the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its progeny laws and regulations, including the Health Information Technology for Economic and Clinical Health Act. 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. When it comes to information security, those requirements include more than 60 required or addressable actions. As HIPAA business associates, law firms can be held directly liable for various HIPAA violations.

Serious civil and/or criminal penalties can be assessed for violations of HIPAA's requirements. Civil penalties can include up to $50,000 per violation with a cap of up to $1.5 million adjusted for inflation after 1996. Criminal penalties can include fines of up to $250,000 and imprisonment of up to 10 years. While not as common as enforcement actions against HIPAA covered entities, the U.S. Department of Health and Human Services' Office for Civil Rights has exercised enforcement actions against HIPAA business associates as well.

- **State 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. 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. 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. In many of these states civil fines and penalties may be levied by state officials for the failure to comply with these requirements. While Pennsylvania has not yet enacted any legislation that require state agency reporting, a 2018 Pennsylvania Supreme Court decision on employer liability for the release of employee confidential information could push the state legislature to consider enacting such laws, and the case set a judicial precedent that in the future could hold companies financially responsible in civil cases for data breaches.

Trends in Cybersecurity in the Legal Profession

In recognition of steadily increasing cyber threats to law firms, the ABA's Legal Technology Resource Center conducted a survey of law firms' information privacy and security preparedness, publishing its results in its annual Legal Technology Survey Report. The report collected information from attorneys in private practice at firms of various sizes on a host of topics concerning the use of technology in the practice of law.

Not surprisingly, attorneys in firms of all sizes voiced significant and increasing concerns over protecting the privacy and security of their confidential information, whether that's information about their firms or the information of their clients. Interestingly, however, the survey results reveal that despite the growing prevalence of cyberattacks on law firms, most attorneys and their law firms lagged behind most other businesses in their implementation of common and effective cyber security defense tools, including tools used by many of their own clients. Cyber criminals, aware of this risk delta, have increasingly pointed their attacks at law firms, considering them "soft targets" from which to obtain valuable, confidential client information.

The report also revealed a growing sense of potential liability among many firms, accompanied by the increased prevalence of cybersecurity risk insurance. According to the report, an increasing number of firms are committing to cyber liability insurance policies, at about 36% percent of the survey's respondents. While

these policies may mitigate many of the costs related to cyber-infiltration, they are far from panaceas. The responsibilities and challenges— and the limitations of insurance—could not be clearer.

What to Do?

While law firms are making progress on cybersecurity measures, many continue taking extreme risks legally, financially and reputationally by not using stronger data privacy protections. If they're not already, law firms should consider promptly enacting data defense tools such as:

- Multifactor authentication to provide better security than just a password (which can be "forced" through algorithms in a matter of seconds).
- Immutable backups to allow a firm to revert to a recent past status in case of ransomware attacks.
- Endpoint detection and response tools automatically monitor all possible entry points to alert cybersecurity staff to any suspicious activity.
- Incident response planning to prepare for when (not if) a firm experiences an attack. Install all updates and patches on all machines accessing company data.
- Employee training on spear phishing, spoofing or other common behavioral attacks.
- Email encryption to ensure confidentiality of communication.
- Whole or full disk encryption on laptops, especially for travel or remote use.
- Cyber insurance to account for financial implications of cyberattacks.
- Remote device management and wiping, especially for remote or travelling employees.
- Device recovery tools to remove any unneeded (and potentially malicious) software web filtering to alert users to dangerous websites, potentially foiling phishing attempts.
- Biometric login to provide another layer of authentication security that is difficult to replicate.

Jeffrey B. Miller *is senior counsel at Saxton & Stump, the chair of the firm's information privacy and cybersecurity group, and director-in-charge at Granite GRC Consulting, a business consulting firm that helps successful firms to optimize resources while managing risk. He counsels clients with timely and practical advice to help them protect their data, improve operations and preserve and enhance value. Contact him at jbm@saxtonstump.com or at 717-556-1088.*