LAWYERS JOURNAL

LAW PRACTICE MANAGEMENT

Fortifying the firm: How to confront digital threats to the modern law firm

By Rachel Aghassi and Ahmed Javaid

The international pandemic caused by the COVID-19 virus has no doubt brought enormous changes, including speeding up the already rapid implementation of technology to the way law firms conduct their practices. Now more than ever, the consequences of data security have become increasingly important given how remote work, digital communications and work product have become the norm. The significance to law firms is magnified due to the type of information and records they typically handle and because of the unique obligations of attorneys.

As lawyers, protecting information is even more crucial because law firms are not only subject to legal requirements applicable to all businesses but must also conform to the professional standards with respect to safeguarding client information, including electronic data. The ABA's Formal Opinion 483 lays out the obligation of attorneys when there is a data breach or cyberattack. It recommends that law firms have an "incident response plan" should a cyberattack and data breach occur that sets forth a clear and precise procedure on how to handle it. Based on the analysis of the ABA Model Rules of Professional Conduct 1.1, 1.6, 5.1 and 5.3, the Opinion concludes that "when a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules." ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 (2018). The commentary to Rule 1.1 of the Model Rules of Professional Conduct further states that a firm should "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."

Accordingly, considering the way modern law firms operate, the challenges associated with handling sensitive data and the special obligations of attorneys, this article provides recommendations in how to prepare for digital threats to avoid them in the first place and what to do when the inevitable happens to minimize the resulting damage to the firm.

Cyber Threats to Law Firms are on the Rise

Cyberattacks against law firms have been on the rise in the last few years. Unfortunately, the reality is that it is not a matter of **if** a law firm will face a cyberattack attack but **when.** Such an attack can result in damage to reputation, interruption in practice and even potential lawsuits arising out of the breach.

In one such case, Millard v. Doran, Index No. 153262/2016 (Sup. Ct., N.Y. Cty. 2016), an attorney was sued by a couple for malpractice arising out of the proposed transaction of a cooperative apartment in Manhattan. During the process, it is alleged that the lawyer violated his duties by allegedly allowing hackers to get into the law firm's emails and obtain communications, which purportedly resulted in the transfer of $1.9 million to the hackers. The litigation records further allege that the breach only occurred because the attorney failed to adequately secure digital communications with clients by failing to take proper precautions, i.e., the attorney failed to install adequate cybersecurity protections that could have prevented such an attack. The case signals that cybersecurity threats can lead to legal malpractice and other claims in the event of a data breach.

Similarly, in another pioneering case, Shore v. Johnson & Bell, Ltd., 16-cv-04363 (N.D.Il. 2016), a class-action lawsuit was commenced against a Chicago-based law firm. The complaint alleges that the firm's computer systems had critical vulnerabilities, apparently subjecting data to impermissible exposure of confidential information. The Shore matter ended up in pre-trial arbitration and likely had issues with establishing damages because the case arose out of claims regarding improper exposure of sensitive client information as opposed to concrete damages from an actual breach. Regardless, these matters underscore and forecast that cyberattacks on law firm infrastructure are very real threats, cannot be ignored and require preventative measures and a game plan for avoiding and dealing with an actual breach.

A hack can have devastating effects on ongoing litigation and complicated business relationships. The firm's reputation can also be damaged, which could hinder the acquisition of new clients who may be leery of potential attacks to their private information.

Due to the severe consequences that can result from a law firm's data breach, it is essential that firms be prepared by implementing data breach protocol before a breach takes place. The difference between an attempted attack and a devastating one will likely be the degree of security implemented by the firm and the type of response that follows. An effective protocol can help secure the information that was sought or limit the potential harm that may be done by unmitigated access to data that should be protected.

Preventative Measures

To prevent cyberattacks in the first place, law firms should be proactive with respect to their cybersecurity protections by implementing the following preventative measures:

1. Assess Needs

The first step should be to assess the nature of the data and records that a law firm possesses to determine what the best and most effective protocol may be under the circumstances. The firm should conduct an inventory of its technology systems, information and software to evaluate and categorize the risk posed by the different types of data. A firm that largely deals with medical malpractice claims will have to ensure that the private health records held are not disclosed with anyone other than those who have authorized access. Similarly, firms handling confidential financial records and tax documents for clients need to ensure that these materials are only available to those individuals, attorneys or others, who should be permitted access to them.

2. Train Staff

After assessing the data security needs of the particular firm, the firm personnel should be apprised of the importance of not sharing confidential information electronically or permitting access to such materials to outside parties without authorization. The protection of information should be addressed with each incoming attorney or non-attorney staff member as part of the firm's policies and included in the firm's employee handbook or guidelines. Employees should be advised through written guidelines and ongoing instructions on the importance of recognizing a cyber threat, how to handle it and to promptly report the threat. Training should include how to recognize and avoid common types of cyber threats such as phishing email scams. Phishing emails and messages tend to be disguised as if they are from a trusted company or source. Disguised as a message from a legitimate sender, the message may seek that confidential information be entered to confirm access or correct issues with an account. However, the information that is exchanged is then possessed by the illegitimate source, thereby providing a means to access additional private data. Attorneys and their staff should make sure that they are actually familiar with the source of electronic communications and whether the information being sought in the message is even related to the nature of the relationship, prior communications or requests. Law firm personnel should be advised to look out for such emails and digital content and avoid taking the bait. They should be knowledgeable about spotting potentially harmful attachments or links and know to report any peculiar messages and requests that they may encounter.

The firm's employees should also be instructed about the proper ways to perform data intake. Whenever information is being saved from emails, online, cloud services or through CDs, USBs or other storage devices, they need to ensure that the source is trustworthy or wait to proceed until it can be confirmed that it is secure.

Obviously, law firms need to be able to share information with their clients, other counsel, experts and other entities. Training should further include teaching employees about what types of records may be shared with those outside of the firm. There should be a procedure implemented to securely share materials that contain confidential information.

3. Implement Safeguards

To ensure that such exchanges do not render the firm susceptible to a cyberattack, a two-factor authentication method can be implemented, which would require two separate authentication methods to access confidential records and prevent anyone without such credentials from obtaining unauthorized access. The specific factors can vary depending upon the level of security required and the resources that can be utilized for the preventative measures. Examples include a password, a PIN number, employee ID number, key card or even fingerprint, eye, voice or face recognition tools. With respect to authentication tools, employees should be instructed on creating effective passwords to protect information on both their work computers and mobile devices. A password management utility can also be implemented for additional safeguards. A firm may want to consider using the principle of least privilege (PoLP), which requires that a user never log in with a level of security above what is necessary for the particular task or job. This method ensures the sensitive information that is accessible and therefore subject to attack is limited.

The precise authentication methods will necessarily vary depending upon the firm's needs and means but having some type of additional safeguards can limit the firm's vulnerability to threats. According to Symantec's Internet Security Threat Report, an industry leader in cybersecurity, approximately 80% of cybersecurity breaches may be prevented if multifactor authentication is in place.

4. Secure Remote Operations

Another potential cyber threat that can arise in law firms is from attorneys or other employees working remotely, which has become extremely commonplace given the international pandemic and many of the resulting changes in work practices will likely be here to stay. All the same protocol and procedures should be implemented with respect to any remote access programs that are used to access files outside of the office. Depending on the firm, it may also be best to limit which employees can access certain data remotely, e.g., only attorneys or certain attorneys have remote access or access should be permitted pursuant to requests made on an ongoing basis.

5. Upgrade Information Technology Systems

On the IT side, law firm IT staff, or IT vendors should regularly communicate with the managing partner(s) about the type of security systems in place, their effectiveness and whether additional protections are required. At a minimum, regularly updated antivirus and firewall protections should be installed. The law firm's IT staff should also have methods in place to conduct regular scans of the firm's digital infrastructure to stay ahead of any threats, recognize the same and pursue actions to remove or limit the effects. It may make sense to have an outside vendor conduct third-party vulnerability scans, penetration tests and malware scans to defend against potential breaches.

It should be noted that no plan will be universally applicable and appropriate for every firm, but the strategies and recommendations discussed herein provide general suggestions

that can be useful. Different firms may have their own specific needs and corresponding requirements. Therefore, it is expected that any protocol will have to be tweaked and fine-tuned to best reflect the specific firm needs, including taking into account the particular threats that may be applicable based on the firm's practice areas, the nature of the client relationships and the resources available to address cybersecurity concerns.

Response Plan

Even the best-laid plans to prevent an attack can still fail. When doomsday occurs, a proper response plan can minimize the adverse effects.

1. Take Charge

First, an individual should be appointed to make everyone aware of the issue and what steps should be taken by those whose accounts have been infiltrated and how to prevent the attack from worsening or spreading to additional files or users.

2. Plug Leaks

In the interim, the firm staff should perform recovery and repair efforts by minimizing the damage done. Recommended actions include changing relevant passwords, authentication methods and potentially terminating the exchange of sensitive materials to the extent practical until the situation is rectified. The termination can also be limited to just the client/files associated with the breach. To the extent that the breach is aimed at the firm's own internal private data, specific departments such as accounting may need to alter or cease certain operations until the security is restored. In cases where information has been lost completely through ransomware, which takes over private data through encryption and holds it hostage, the firm should immediately ascertain whether backup data can be accessed and in what form.

3. Notify Others

Additional steps to take include contacting other counsel, court personnel and/or the applicable cyber insurance company. Depending upon the size of the breach, the firm may need to notify relevant law enforcement agencies to coordinate potential investigations. In some instances, it may also make sense to retain a data breach lawyer or a digital forensics company. This may have to be done through other means if the normal email and phone communications can no longer be safely accessed. Appropriate backup options need to be considered beforehand.

Furthermore, the firm may need to take necessary steps to notify individuals outside the firm whose information has been compromised. Although it may not ever be a conversation that a firm wants to have with a client, pursuant to applicable State, Federal or Professional requirements, it may be necessary for the client to be advised of the disclosure of private information not only so that the firm complies with legal and ethical obligations but so that the client can also be proactive and take steps to limit the potential damage. In addition, the client may be able to provide assistance with executing the incident response plan in the form of additional resources to safeguard information, including alternative authentication methods to continue with the representation as necessary. All of the foregoing should also be documented as written records of the response will be useful for any related investigation, insurance coverage or potential legal action.

Conclusion

As set forth above, the digital threats faced by the modern law firm are palpable and constantly evolving in an increasingly digital workspace. Lawyers should therefore "employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data and the use of data." ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 (2018). Firms should also seriously consider procuring a law firm cyber insurance policy that can bridge the gap and avoid serious complications with the firm's practice while the security breach is being addressed and hopefully resolved. Notwithstanding, at a minimum, law firms need to be proactive in making preparations for the threats they will inevitably face, continue to monitor them, update their protections accordingly and train their attorney and non-attorney staff how to best handle and confront these rapidly developing digital security issues. ■

This article was prepared by Rachel Aghassi and Ahmed Javaid of the New York City-based law firm of Furman Kornfeld & Brennan LLP. For more information about the above topic or the authors, please visit www.fkblaw.com. *We trust that the above article was useful and thought-provoking; however, please note that it is intended as a general guide and opinion only, not a complete analysis of the issues addressed, and readers should always seek specific legal guidance on particular matters. For more information on LPL coverage generally, contact USI Affinity today.*