Are Hackers Secretly Stealing Your Practice?

By David J. Shannon and R. David Lane, Jr.

The Legal Intelligencer – Cybersecurity Supplement
June 23, 2015

How times have changed. Five years ago, most people had never heard of a data breach. Two years ago, everyone was talking about the Target data breach. Today, we are accustomed to news reports announcing data breaches on a weekly basis. The world has become surprisingly numb to the public announcements of lost personal information and health care records that are the result of human error or cyberhacking attacks.

However, the significant legal and financial consequences of a data breach and the failure to notify the public have never been greater. State attorneys general, the Department of Health and Human Services, credit card companies and banks are all actively enforcing laws, regulations and contractual obligations to recoup the millions of dollars lost in data breaches.

Law firms, like all businesses, receive and store significant amounts of personally identifiable information and personal health information. Just like other businesses, law firms can suffer a breach through human error, phishing scams or other cyberattacks. As the owner of clients' confidential personal and legal information, law firms have a special obligation to protect this data.

Data Breach Notification Laws

Law firms have always been aware of the legal and ethical obligations to keep clients' confidences. However, in the event of a data breach, a firm must also determine its obligations under data breach notification laws that may be in effect in the firm's jurisdiction. Today, 47 states have laws requiring some form of breach notification.

Most state laws are modeled after California's security breach notification statutes, which were the first in the nation in 2002 and continue to influence other states' policies with regard to personal privacy protection. State statutes contain requirements regarding notification to the affected consumers and the state attorney general or consumer reporting agencies based on the number of individuals affected. However, variations among the state statutes do exist. For instance, the Massachusetts statute requires that notification to the attorney general and Office of Consumer Affairs and Business Regulation includes, among other things, the number of Massachusetts residents affected and whether law enforcement is engaged in investigating the incident.

In Pennsylvania, data breach notification is governed by the Breach of Personal Information Notification Act. Like other breach notification statutes, the act

requires that "an entity that maintains, stores or manages computerized data that includes personal information provide notice of a breach to any resident whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person." Except under certain exceptions provided for in the statute, the notice required under the statute must be made without "unreasonable delay."

Interestingly, unlike many other jurisdictions, the act does not require an entity to notify the attorney general or other government official of a breach. However, the Pennsylvania Attorney General's Office can contact an entity when it becomes aware of a breach to request information. A law firm should prepare for such a call and inquiry if a breach has occurred, particularly if the breach is publicized or a significant amount of notification letters have been mailed to Pennsylvania residents.

Addressing Data Security and Breach Response

Ensuring compliance with data breach notification laws is not going to solve all of a firm's problems in the event of a breach. Experts readily acknowledge that law firms can be attractive targets for hackers due to the wealth of sensitive information that firms maintain, including business and trade secrets, personal financial information, Social Security numbers, medical records, and privileged legal communications. Even when a breach is not the result of an outside attack, the inadvertent leak of sensitive client information can result in a breach and harm both the firm and its clients. Therefore, law firms must strive to safeguard their data in an effort to prevent a breach in the first place. If a breach does occur, a firm must also be prepared to mitigate the damage.

In an effort to prevent data breaches, firms should create a data security team composed of individuals who can set up and maintain network security and ensure compliance with legal requirements and best practices in safeguarding information. C-suite management, in-house and outside counsel, public relations, human resources and information technology and security personnel should all be represented on the data security team. The team should determine the kinds of data the firm stores and where it is stored, be it on the network, in electronic form residing on equipment or mobile devices, off-site with a cloud service provider or in hard copy. The firm should routinely manage the amount of data that it stores by purging old data to reduce the amount of sensitive information that could place the firm at risk in the event of a breach.

The team should also develop a data protection plan designed to prevent breaches and respond to a breach. Holding regular data security training for individuals who work at the firm helps to prevent breaches by making those individuals aware of the risks and consequences of a breach and requiring them to comply with procedures designed to prevent a breach. These procedures include Internet and email usage rules, document destruction procedures, and third-party disclosure protocols. It is important that the team routinely reviews and updates its security plans to take into account the latest legal requirements and technological advances. With the average cost of a data breach now

up to $3.8 million, according to a 2015 Ponemon Institute study, law firms of all sizes may also benefit from obtaining cyber and privacy insurance containing appropriates types and levels of coverage in the event of a breach.

If a breach does occur, in addition to complying with breach notification laws, a law firm should consider offering credit monitoring services to potentially affected individuals, even in instances where credit monitoring is not required by statute. For law firms that have appropriate cyberinsurance, the services of a credit monitoring agency will likely be covered and normally include free credit monitoring, a call center available for questions and advice and the added benefit of identity theft insurance protection. Breached entities typically offer these services at no cost for one or two years.

Necessary Procedures

The main takeaways for a law firm preparing to address data security and proper data breach response procedures are:

- Create a data security team.
- Determine what data you store, how and where.
- Develop a data protection plan.
- Purge old data.
- Conduct regular data security training.
- Routinely review and update your security plans.
- Obtain cyber and privacy insurance.

As data breaches proliferate across the country, law firms must understand the risks of a data breach and how to prevent them. By making security a priority, law firms can prevent or minimize a data breach and its consequences. Hackers are lurking in all areas of the Internet, and a law firm not properly preparing is putting at risk its own data and that of its clients.

David J. Shannon *is co-chair of the privacy and data security practice group at Marshall Dennehey Warner Coleman & Goggin. Contact him at djshannon@mdwcg.com.*

R. David Lane Jr. *is an associate in the practice group and can be reached at rdlane@mdwcg.com.*