NOVEMBER 21, 2016

Legaltech© news

ONLINE

An ALM Publication

6 Steps for Law Firms to Minimize Damage in a Data Breach Up-Front

From governing data storage to educating employees, getting prepared doesn't need to be reactionary.

BY IAN RAINE

It is easy for domain credentials to get into the hands of criminals. With one successful phishing hack, all of the confidential content that the victim has access to—their inbox, the firm's document management system, network file shares, and so on—can become compromised. Legal and financial services professionals are especially vulnerable; as research shows the chances of these firms being targeted by cybercriminals is upwards of 95 percent. Even with excellent perimeter security in place, it is highly likely that your firm has already been compromised. Whether by malicious actors outside the organization or within, the bottom line is your clients' private information is constantly at risk of being exposed.

To limit losses as much as possible, it's important for law firms to change their mindset from one of prevention to one of containment because no security system is perfect. Only by being prepared ahead of time and having the right operational standards in place, can you and your clients be confident that when a hacker does get in, they'll find very little and they'll be identified quickly. By following these six steps, you can achieve a level of preparedness necessary for minimizing damage from a data breach.

Credit: Lagarto Film/Shutterstock.com

1. Store data in governed locations: When it comes to protecting your clients' data, where you choose to store it plays a critical role in keeping information out of the wrong hands. Governed locations such as document management systems offer significant benefits over ungoverned ones such as network file shares. These benefits include:

- Multi-factor authentication;
- Matter or client-specific security levels;
- Encryption of data both at rest and in motion; and
- Tracking user access through audit trails.

Storing the bulk of client data in simple file shares or email inboxes, while temptingly convenient, simply will not offer the same protection and is best to be avoided.

2. Adopt a more stringent security model: Pessimism can often be taken as a negative in the workplace; however, in matters of security it is actually quite useful. You can identify your organization's security mindset by asking a few simple questions: Does everyone in the firm have the same level of access to information? Or is access determined based on attributes such as matter specificity? If you answer yes to the former, your firm is operating under an optimistic security model, which means potential hackers are likely to do much more damage in a security breach. If the latter sounds more familiar, then you are operating under a pessimistic or need-to-know model.

This is certainly the attitude toward which we see our industry moving, and rightly so. By giving everyone in a firm—from an intern to the senior attorneys—access to just the information they need to complete their job, the firm and client data will be much more secure.

3. Using secure file sharing tools: Collaboration and communication are an essential part of servicing clients. Many professionals rely heavily on email applications such as Outlook to complete these tasks, sharing sensitive documents back and forth for review and feedback. Each time information is shared this way it adds to the risk: As more people are included in an email chain, more access points become available to hackers.

An effective solution to this is to use a sharing tool that integrates with your workflows and your content creation applications, allowing you to share, edit and collaborate securely both in the office and on-the-go. Not only do these tools keep information governed and monitor who is accessing the files, they can also deliver significant productivity benefits.

4. Enforcing data retention policies: Another fundamental part of minimizing damage in a data breach is having a central policy for tracking, retaining and disposing of client information once it has reached end of life. Of this group, the disposal policy has arguably the highest potential to keep data out of harm's way, yet it is often the most ignored.

Why? Professionals tend to save everything in case it's needed for future reference. This is understandable, but over retention is incredibly risky for your business and increases potential exposure to hackers. Take for example Firm A and Firm B. Firm A has no retention policy and never deletes anything, whilst Firm B's default retention policy mandates data disposal five years after matter close date. If Firm B is attacked, then the amount of data that is at risk is clearly going to be a lot less than that at Firm A.

5. Using machine learning to detect unusual activity: Two technologies that are helping to change the way businesses operate are analytics and machine learning. With the right software product, law firms can keep track of data in unprecedented ways, including monitoring usage and access for a-typical patterns. This kind of observation is key to reducing the average time taken to expose cyber criminals, which research tells us is currently more than 150 days. Firms can also configure trigger points or "booby traps" to help alert professionals to malicious activity before it gets out of hand. Best of all, machine learning tools become smarter the longer you use them.

6. Educating employees: The final and most important step for keeping breaches contained is educating employees at all levels. The weakest link in an organization's security plan is its people—not (necessarily) because they are malicious, but because they are uninformed. Professional development classes on security threats are a good start, but these should be supplemented by phishing email tests with follow up information about what has occurred and how the employee should have responded.

At the end of the day, encouraging the right security-conscious mentality throughout the organization and creating a culture of reporting that rewards people for speaking up are what will truly make a difference for your firm. With these steps in place to help safeguard information, hackers will find it so much more difficult to profit when they breach the outer perimeter and will quickly focus their efforts elsewhere.

***Ian** has more than 25 years of experience in the IT industry, building information governance and records management software products for the enterprise. He is currently head of product management for the iManage Govern division, responsible for iManage's suite of information governance products for professional service firms.*