Do you know why thousands of law firms see their retirement plan in a different light?

Because they've chosen a different kind of 401(k) provider.

The **ABA Retirement Funds Program** ("the Program") is an employer-sponsored 401(k) plan uniquely designed for the legal community. For over 55 years, we have been committed to our mission of providing the tools necessary for all law professionals to achieve retirement security.

What makes us so different?

Oversight: Highest level of fiduciary oversight allowable through ERISA, saving your firm time and reducing your fiduciary risk.

Investments: Investment platform with options to allow for optimal choice and flexibility for your participants.

Service: Fully bundled service model, custom designed to meet the unique needs of the legal community.

The Program is structured to provide affordable pricing whether you are a Solo Practitioner or a large corporation.

Getting started is easy. Contact us today!

ABA
Retirement
Funds

A different kind of retirement plan

☎ 800.826.8901

🌐 www.abaretirement.com

✉ joinus@abaretirement.com

ALA® VIP
Value in Partnership

The ABA Retirement Funds Program is available through the Association of Legal Administrators, an ALA Value In Partnership Program Provider, as a member benefit.

Please read the Program Annual Disclosure Document (April 2018), as supplemented (March 2019), carefully before investing. This Disclosure Document contains important information about the Program and investment options. For email inquiries, contact us at: joinus@abaretirement.com.

Securities offered through Voya Financial Partners, LLC (member SIPC).

Voya Financial Partners is a member of the Voya family of companies ("Voya"). Voya, the ABA Retirement Funds, and the Association of Legal Administrators, an ALA Value In Partnership Program Provider, are separate, unaffiliated entities, and not responsible for one another's products and services.

CN700696_0121-2019

ANN NICKOLAS

How Law Firms Can Train Employees to Protect Client Data

In 2017 alone, more than one in five law firms experienced a data breach, proving the need for heightened protection of customer data in law firms across the nation. Not only is protecting sensitive information essential in compliance, but it also impacts client loyalty. In fact, 83 percent of Americans say that security is a contributing factor when deciding which law firm to work with.

> “Thirty-seven percent of law firms that experienced a breach reported a loss in billable hours, and 28 percent incurred hefty fees for correction.”

Outside of client loyalty, firms should be concerned with the impact a data breach will have on their bottom line — 37 percent of law firms that experienced a breach reported a loss in billable hours, and 28 percent incurred hefty fees for correction. Yet, most law firms do not have information security protocols or employee training in place to safeguard physical documents and electronic devices that contain clients' confidential information. Namely, one in four law firms (26 percent) have never trained their staff on information security policies or do not have information security policies in place.

Law firms are going through a modernization to improve the client experience, but this comes along with new challenges and new threats to clients' confidential information, as well as new processes for employees. As of 2017, 95 percent of law firms were not compliant with their data governance and cybersecurity policies. With sensitive information — as well as business on the line — there's no question that law firms need to implement a strategy to step up their security policies, and this strategy includes a major training overhaul for employees. Let's explore how law firms can train their employees to help protect client data.

TRAIN EARLY AND PROVIDE REINFORCEMENT

Waiting for a data breach to occur in your firm is the wrong strategy when it comes to teaching employees security protocols. If possible, incorporate a training process into your onboarding process for new hires, and hold all-staff training sessions on a regular basis to update employees on new protocols and remind them of current policies. Using real-world examples and practical tips for information security is the key to keeping employees engaged in the training, as it provides context for the gravity of data breaches and helps employees retain the training information.

PROVIDE GUIDANCE ON NEGLIGENCE AND DOCUMENT DESTRUCTION

The more employees a law firm has, the higher the risk of employee negligence that may cause a data breach. Employee training for data security must include teaching employees how to identify negligent, unethical or malicious behavior, while also encouraging them to take action if client data is at risk.

In addition to training employees on negligence, firms must consider the everyday physical security risks that come from the large amount of personal information they store about witnesses in litigation. Providing policies and training that guides employees to conduct consistent clean-outs and destroy outdated documents, as well as hardware containing data, can be coupled with already occurring employee training. For documents to be properly disposed, they should be shredded rather than just recycled. For hardware, there is a frequent misconception that merely wiping the device is enough to destroy the information it held. However, the best way to train employees to securely dispose of hardware or hard drives is to have them destroyed by a professional.

DEVELOP A POLICY FOR REMOTE WORKERS

Eighty-six percent of C-suites and 60 percent of small business owners agree that the risk of a data breach is higher when employees work off-site than when they work at the office. Yet, more than half of lawyers at the top law firms in America now work remotely at least some of the time, providing unique challenges for information security policies.

With remote work becoming a growing trend in the legal industry, law firms must develop and train employees on remote work policies in order to keep the risk of a security breach down, while keeping employees happy. Working with your IT team to develop a remote working infrastructure, such as a secure VPN to remotely access data, and ensuring the team will be available to support remote workers, are good first steps in creating a policy. Firms should also create a policy for physical documents when working remotely — for example, keeping sensitive documents in a locked briefcase while traveling. Training employees on these policies through a combination of guides, town halls, emails and in-person walkthroughs will help ensure all employees understand the plan.

There is no understating the damage that a breach can do to a law firm and its clientele, but the good news is that there are many processes that firms can put in place to prevent a breach from happening. The top of the list is to train employees on these policies and make them your first line of defense against a breach, rather than risk them being the reason it happens in the first place. ■

ABOUT THE AUTHOR

Ann Nickolas is Senior Vice President at Stericycle, provider of Shred-it solutions, where she oversees new business development and account management for customers in the commercial, health care and government verticals. Nickolas helps businesses secure their confidential information with products, services, policies and training that help protect them from the risks, fines, penalties and loss of revenue that come with an information breach.

www.shredit.com