How Small Law Firms Can Improve Cybersecurity to Prevent Data Disasters

By Josh Taylor, Smokeball

Insufficient data security practices lead to devastating consequences for small law firms. Breaches can inflict irreversible damage to a firm's reputation, finances and client relationships. So why aren't they taking cybersecurity seriously?

A recent American Bar Association survey uncovered this lack of concern, finding that only 42% of firms took action to increase digital security measures last year. Of these, 27% did so to better protect client or contract data. While lawyers spend their time looking out for clients' risks and liabilities, the data suggests this diligence doesn't extend to internal matters.

Exactis' 2018 data leak shows how small business security lapses balloon into a much larger crisis. This breach exposed the personal information of over 230 million people and 110 million businesses, demonstrating that even smaller-scale businesses store massive amounts of sensitive data and face a constant threat as their data pool grows.

While small law firms may not have a long roster of big-name clients, they store a significant amount of personal details and business information. Clients trust them to protect sensitive business information like proprietary data, financial details and confidential deals. Leaks and breaches have severe ramifications, causing clients to walk out, IT headaches, financial worries and regulatory violations.

An accident or technical error may have created the breach,

but innocent causes don’t render firms immune from serious business consequences. Each law office is responsible for preventing and quickly responding to leaks or attacks. Technical aspects of cybersecurity may overwhelm some small firms, but improving data protection and online safety practices doesn’t have to be complicated. Law firms bolstering digital security can start by keeping in mind a few simple tips:

Make Security People Powered

Small law firms don’t often face the organized cyber threats that plague larger organizations. Their risks tend to lie within the firm itself, stemming from workers that lack the technological savvy to sidestep malicious schemes. Ransomware and phishing scams rely on human error, and untrained employees open the door for them to poach important private records.

Implementing regular training for all employees assists organizations in avoiding personnel-caused breaches. This way, staff stay updated on how best to protect themselves and the firm from nefarious email schemes and other tactics cybercriminals use to siphon off personal data. Additionally, law offices should cultivate channels for quick information distribution to allow employees to respond quickly during data leaks. Training programs may increase costs and responsibilities up front, but pay off later on by warding off detrimental security issues.

Invest In Updated Tech

The phrase “small law office” doesn’t typically conjure up images of futuristic operations and state-of-the-art technology. But more than hurting firms’ reputations, this digital sluggishness produces security risks. Offices running on inconsistent operating systems, outdated software and unsecured Wi-Fi networks take on a higher vulnerability.

Fortunately, these technology issues are easily fixed. Scheduling regular hardware and software updates and frequently changing the internet password helps fortify firms' defenses.

Though it may seem obvious, it's worth noting the large role passwords play in ensuring smaller firms' security. One weak link opens the floodgates to your entire database of client information. Keep login information for sensitive data on a need-to-know basis, and consider using a password manager for all employees. Frequently changing passwords, though a small step, provides another line of protection against cyber threats.

Reduce In-Office Risks

Traditional, lock-and-key security is an easy concept to grasp, but digital security is a hazier concept. Fortunately for firms not familiar with technology-driven data protection, the two share some common ground.

Some believe that on-site servers make data safer, but this is a misconception. Seeing storage equipment physically in the office may be reassuring, but centralizing this information just compounds the risk. For example, burglars breaking into a small law firm could then take much more than basic office hardware. Backing up and housing data in the cloud lowers this hazard for organizations, removing important data from the risks inherent in physical spaces.

Another seemingly innocuous practice that poses security issues is carelessness with paper documents. More firms are adopting digital document software, but paper remains popular at many small firms. These documents also expose confidential information if left in plain view or accidentally included in social media photos. Just like with digital risks, reminding employees of security best practices helps suppress future issues.

Just like any business entrusted with sensitive data, law firms must commit to shielding themselves and clients from data breaches. Leaks at small offices quickly expand into a big problem. As data storage demands continue growing, firms can introduce simple technology and security improvements that protect client information and preserve their reputation.