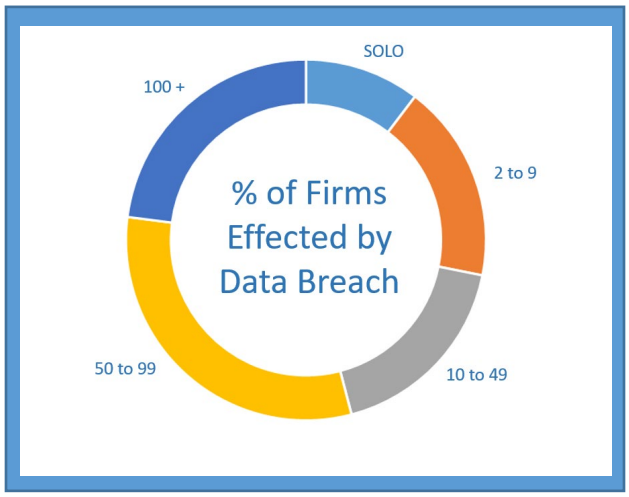
CYBERSECURITY IN LAW FIRMS

LAW FIRMS ARE TARGETS.

Recent news has revealed that law firms are a wealth of private information and are overwhelmingly unprotected. From client information to employee data, law firms continue to be a gateway for socio-political exploitation. These types of attacks don't just leave information vulnerable, it damages reputation, wastes time and loses clientele. In 2012, Robert Mueller, then-FBI director was quoted:

> *"I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."*

Since 2012, trends in data security are frightening, no longer are large enterprise the only target, it small businesses, small firms are a great resource to hackers. Cybersecurity no longer encompasses just changing passwords or updating a firewall. Cybersecurity is an extensive set of standards and often daily rituals that protects firms and clients alike.



FIRM'S VULNERABILITIES VARY

The American Bar Association reports that while 40% of all law firms have been previously infecting my malware, viruses or various forms of cybercrime, firms from 10 to 49 persons in size have a much higher rate of infection at 57%. In all of this, only 14% of firms report those crimes to law enforcement officials.

CYBERSECURITY IN LAW FIRMS

According to the ABA Tech Report 2018 only 36.2% of respondents from firms of more than 500 lawyers said "yes" to cloud usage. Those who do adopt cloud technologies enjoy 24/7/365 anywhere access, lower costs and data security much greater than what firms can provide on their own. Cloud migration can seem daunting and often costly move.

Looking to the Panama Papers breach, email encryption, or lack therefore was the catalyst from which over 100, 000 documents were compromised, violating not only client-attorney privilege, but also was described by Edward Snowden as the “biggest leak in the history of data journalism” via Twitter. The firm lost money, reputation and stands today only as a case study of what not to do in the realm of legal cybersecurity.

The internal realities of a data breach can be described in cost of downtime. According to Attorney at law magazine, if a firm with 25 employees who bill at $200 per hour each lose one hour of uptime per month, that’s $60,000 a year on lost opportunity for a firm operating on billable hours. This cost only includes tangible asset loss and does not take into account time and lost reputation.

REPUTATION IS EVERYTHING. Time is money. With cloud computing, reputation and time are preserved when the inevitable strikes.

The precautions that firms can put into place are numerous. Cloud migration serves has a fundamental step to security, and offsite backups allow for data restoration prior to attack, often in as few as 15 minutes. This accessibility grants firms the ability to rewind the clock to before disaster struck and recover data and allow business continuity.