January 28, 2019 **TECHREPORT 2018**

2018 Cybersecurity

David G. Ries

Share this:

Security breaches are so prevalent that there is a new mantra in cybersecurity today—it's "when, not if" a law firm or other entity will suffer a breach. In an address at a major information security conference in 2012, then-FBI director Robert Mueller put it this way:

> "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."

Mueller's observation continues to be true today for attorneys and law firms as well as for small businesses through large global companies. There have been numerous reports for over a decade of law firm data breaches in the popular and legal press—print and online. The FBI has reported that law firms are often viewed as "one-stop shops" for attackers (with information on multiple clients) and it has seen hundreds of law firms being increasingly targeted by hackers. Law firm breaches have ranged from simple (like those resulting from a lost or stolen laptop or mobile device) to highly sophisticated (like the deep penetration of a law firm network, with access to everything, for a year or more).

New York Ethics Opinion 1019 warned attorneys in May 2014 about this threat environment:

> "Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and

ABA American Bar Association |

/content/aba-cms-dotorg/en/groups/law_practice/publications/techreport/ABATECHREPORT2018/2018Cybersecurity