New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 259—NO. 46
FRIDAY, MARCH 9, 2018

IN THE LAW FIRMS

Cybersecurity: NY's Midsize Law Firms to Face Increased Scrutiny

BY SUSAN DESANTIS

NEW YORK'S midsize law firms are feeling the heat when it comes to cybersecurity.

Facing scrutiny from regulators, clients, adversaries and peers, midsize firms are taking action like never before. But experts say the sensitive data they store is still vulnerable to hackers who seek to blackmail firms, investors who want to profit from insider trading and thieves who are out to steal escrow accounts.

"I think it would be hard to find a New York firm of any size that isn't feeling the heat from their clients and hasn't taken some kind of action." said Jason Straight, senior vice president of cyber risk solutions for UnitedLex Corp., which advises law firms and other clients out of its offices in downtown Manhattan. "The midsize firms just have a lack of understanding about how to approach these issues."

Big banks put the pressure on Big Law first when concerns about cybersecurity came to the forefront several years ago. But now, midsize law firms that have successfully competed for some of that business since the recession will lose those clients if they don't meet the same cybersecurity standards as the big firms do.

Jason Straight is a cybersecurity expert at UnitedLex

The New York State Bar Association, along with its counterpart in New York City, has taken notice and is working to get its members educated. Since the beginning of 2017, the state bar association has presented 10 cybersecurity CLEs and about 500 lawyers have attended.

"A lot of law firms think no one is going to do that to me but that's not the case. It's happening all over the place," said Marian Rice, who as the chair of the New York State Bar Association law practice management committee is partly responsible for the educational programming.

In her practice representing lawyers involved in malpractice and disciplinary matters at L'Abbate, Balkan, Colavita & Contini in Garden City, Rice began seeing cybersecurity cases eight years ago. The most common type involved funds being misdirected into the accounts of thieves pretending to be clients or adversaries. While it was possible to claw back some of the ill-gotten gains, attorneys did lose clients' money, she said.

John Sweeney, CEO and managing partner of LogicForce, which puts out a law firm cybersecurity scorecard every quarter, said midsize firms do have some catching up to do.

"One thing I would say about midsize v. Big Law, they're very customer-focused but at the same time with regards to the sophistication and investment necessary for what we believe to be best practices at a well-run law firm from a cybersecurity viewpoint, they're a little behind," Sweeney said.

Of the law firms evaluated in the fourth quarter of 2017, 62 percent were small or midsize with fewer than 150 lawyers. The report specifically warns such firms to take the threat seriously.

"Law firms should not take comfort in thinking they may be too small or remote to be victimized. The event that impacted DLA Piper and innumerable other businesses would likely have affected thousands of law firms in the U.S. if it wasn't primarily a regional event," the report stated.

LogicForce evaluates law firms against 12 standards, all of which its leaders consider necessary for true cybersecurity.

Compliance was low: Only 43 percent of the firms have documented policies and procedures, 42 percent conduct some type of penetration and vulnerability testing, 41 percent have cybersecurity insurance, 38 percent have a credentialed information security executive, 32 percent make staff training mandatory and 30 percent have multifactor authentication.

Of those that have designated a person to handle cybersecurity, the experts say the firms often choose the wrong person. Sometimes it's a partner who is more focused on bringing in revenue than cybersecurity or an IT director whose main responsibility is making sure that lawyers can log in from the beach, the train or the airport.

"When a partner's primary responsibilities or pressures are servicing the client and bringing in revenue, how much time can they spend on the cybersecurity of the firm?" Sweeney asked.

Luise Barrack, managing member of Rosenberg & Estis, a New York real estate firm with about 80 attorneys, said a hacker recently got into an adversary's escrow account and switched the wire transfer information. The impostor communicated with a Rosenberg & Estis partner for a couple of weeks and tried to get the escrow money sent to the wrong account. The adversary discovered the hack because while the forgery was good, it wasn't good enough, Barrack said.

"Think about it. It's huge. If you can get into law firm's escrow accounts. Who else has that kind of monies that are being transferred?" she said.

Ronald Shechtman, managing partner of Pryor Cashman, a New York City firm with about 170 lawyers, said there was a similar attempt on his firm. The firm, handling a substantial deal, was asked to send a couple of hundred thousand dollars to an account in the Far East.

The attorney asked for written confirmation and got back a fax from the client on his unique stationery with his unique signature.

"Luckily the account number was wrong or something was wrong on the number," and the transaction didn't go through, Shechtman said. The attorney called the client to apologize for the mistake and that's when it was discovered that the client's email had been hijacked.

"The first lesson is that written confirmation isn't enough," Shechtman said. "But in terms of the basic cybersecurity protections that you need it's just not an area where you can economize."

Richard Haddad, who is chair of the litigation practice at Otterbourg, a 50-attorney law firm in New York City, has been in charge of technology issues since he was the youngest partner 19 years ago.

"We have our IT director meet with the cybersecurity teams of the major financial institutions that are our clients," Haddad said.

The clients make recommendations on whether attorneys should be allowed to access social media from their work computers, whether the staff can check email from work and whether attorneys can cut and paste from the network into email.

"We're shutting a lot of that down and we're restricting the ability to do certain activities remotely," he said. "Some lawyers don't like the inconvenience but I liken it to you have to take off your shoes to get onto the airline. You didn't used to have to do this but that's part of the process."

He gets reports about attempted threats against the firm every week. "We have thus far been able to prevent any damage to the firm or the clients," he said.

Asked if cybersecurity keeps him up at night, he said, "What keeps me up is the argument I'm going to make in court."

@ Susan DeSantis can be reached at sdesantis@alm.com. Twitter: @sndesantis