NetDiligence®

‹ Back To The Blog

Cyber Risk and Law Firms

Cybersecurity / January 13 , 2022

Like many SMEs, law firms have proven to be low-hanging fruit for cyber attackers, with the American Bar Association reporting that 29 percent of smaller law firms have experienced a data breach—up from 26 percent the previous year. Yet law firms, which routinely handle sensitive client data, are subject to data security and privacy laws such as New York's SHIELD act and California's Consumer Privacy Act. We spoke with Ondrej Krehel of LIFARS about how and why law firms are being targeted and what they can do to shore up their defenses.

What are some of the cybersecurity risks that law firms are facing?

We've seen an uptick in law firm attacks, probably about double the cases we used to see just here at LIFARS, especially those dealing with real estate transactions. Threat actors are increasingly picking law firms that are wiring money in and out and targeting them for BEC (Business Email Compromise) attacks. These attacks attempt to re-direct funding to the wrong account. Inquiries are coming through what we call our Cyber 911 with individual victims asking for help.

Usually, some time has passed (about a week, sometimes longer) and by the time the victims reach out for assistance it is often too late to do anything (from an incident response point of view). Of course, the representative from the law firm seems ashamed that it happened, and they don't provide much guidance to victims about what to do next. It seems that in many cases these victims are afraid to go back to the law office and say, "Look, it was your system that was compromised. You need to give me back my money."

Would you say that wire fraud schemes, in general, are on the rise, or is it just that they've zeroed in more frequently on this target? And why law firms? What is the weak link here?

I'd say that perpetrators are specifically zeroing in on law firms to commit business email compromise, which right now is the second most common attack/hack, with the first being cyber extortion ransomware. If you look at the statistics, typically the threat actor(s) find a way in through the law firm's cloud platform or email servers on these platforms. The unfortunate reality is that many law firms are in denial that this can happen to them, until it does.

What can law firms be doing to avoid attacks on this particular front?

should not be able to access the cloud or email system and multiple sessions should not be allowed. For example, you can't have a session from Ukraine at the same time you have a session from Chicago.

In the case where law firms have implemented two-factor authentication, threat actors still may have a way to circumvent it, so law firms really need other security controls like strong certificates in place to bolster their readiness.

Are endpoint detection and response systems useful for a law firm?

Any company should have an endpoint detection and response system, but I think law firms especially should really consider hiring a third-party security provider to assist, particularly since law firms can be dealing with highly sensitive data. You can implement all the right technology, but you need humans to help you monitor the situation and ensure that the technology is working.

What are the stakes involved for a law firm hit with a business email compromise attack?

They could be liable for those lost funds if their system is compromised. Law firms should be insured to pay for these costs, and they should strive to help the victims quickly. But that is not happening nearly enough. For example, the law firms that we dealt with in upstate New York took two or three weeks to notify the victims. And in some cases, the victims are not getting their money back and that's not the right thing to do. The damage that BEC causes not only hurts financially but it also can destroy a firm's reputation which can affect future business.

Elisa Ludwig

Share

Sign Up for the NetDiligence Newsletter

Stay informed about the latest cyber news & events.

Email*