Clients Turn Up the Heat on Cybersecurity

Expectations and regulations aren't getting any easier to deal with. Here's how your firm can learn to stand the heat and stay in the kitchen.

MARK BREWER
Freelance Writer

Cybersecurity has been a hot topic for law firms for some time. But as regulations and other requirements grow, clients are ratcheting up their expectations for law firms to keep their data secure.

According to James Harrison, Chief Executive Officer of INVISUS, a cybersecurity company with law firm experience, law firms that do business with regulated companies are considered business associates, and business associates that hold client data are, under law, subject to the same data security requirements as the businesses they represent. If a law firm is compromised, the client must answer to regulators.

"So there's downward pressure on law firms from the marketplace to evaluate their compliance with best practices in data security and privacy," he says.

THE INFORMATION SUPPLY CHAIN

Law firms are expected to follow best practices that stem largely from state, federal and international laws. Law firms holding data from health care organizations must follow HIPAA

"There's downward pressure on law firms from the marketplace to evaluate their compliance with best practices in data security and privacy."

regulations. If they host data on European Union citizens, it must be handled in accordance with the General Data Protection Regulation (GDPR). There are also requirements under the Gramm-Leach-Bliley Act and new regulations for financial services companies from New York's Department of Financial Services.

Some clients may have additional requirements under their general liability or cybersecurity insurance policies. And all 50 states have legal requirements on how companies must respond to data breaches.

And if you use a third-party company for IT operations or store client information in the cloud, these vendors are also considered business associates and must comply with your clients' requirements. So it's up to law firms to vet their vendors.

"We call it the information supply chain," says Harrison. "If you look at the flow of data — who touches it and has access to it — you need to follow that trail and verify that everyone is following the same best practices."

MORE QUESTIONS THAN ANSWERS

Proof of compliance is one expectation that's breathing down the necks of law firm leaders. Law firms are required to complete long, detailed technical questionnaires to do business with many companies. Some require on-site audits, forcing law firms to show higher levels of compliance and proof. "It's sweeping the legal industry," Harrison says. "If a law firm hasn't seen a questionnaire or audit, it's just a matter of time before they start seeing them on a regular basis."

Many law firm management professionals are simmering with frustration over these requests and are at a loss to answer many of the questions. Others have had time to adapt.

"I spend hours and hours on it every week," says Lori Hughes, ALA's Region 5 Director and the Lead Operations and Information Security Officer at Miller Nash Graham & Dunn LLP, a law firm with 160 attorneys in three states. She has been answering questionnaires since 2015 — on HIPAA compliance, insurance requirements and, more recently, cybersecurity.

One questionnaire included more than 300 questions in just one section. And the questionnaires and audits have been snowballing — Hughes says Miller Nash started with about a dozen in 2015; they now see more than 50 per year.

While you may be tempted to pass audits and questionnaires off to your IT department or vendor, less than 50 percent of these evaluations are IT-related, according to Harrison. Cybersecurity requirements now touch human resources, facilities and firm management. The days of cybersecurity simply being a matter of IT applying security patches are long gone.

Hughes says that requirements may include physical security, such as having paper documents in locked rooms, clean-desk policies and guest badges that time out. Many want copies of firm policies, incident response plans and disaster response plans. On the technical side, companies expect features like encryption of laptops and drives, intrusion detection and response, anti-malware capabilities and penetration testing. Many companies require security awareness training for all firm employees.

BEAT THE HEAT WITH A PROCESS AND PLAN

"Cybersecurity a moving target. It's not something you can set and forget," Harrison says. "What happens the next time you land a key client and they have a new type of data they intend to share with you?"

Unfortunately, as client expectations increase and regulations evolve, law firms are often left in the dark about how to navigate this dynamic landscape. But specialized expertise can help them avoid turning cybersecurity into a daunting and costly task.

Harrison counsels clients not to overkill compliance. "Develop a formal plan that is simplified to the needs, size and scope of the firm and that meets the core of the cybersecurity standards," he says. "That way you can afford it, manage it well and be defensible." Being defensible against a client audit

Cybersecurity requirements now touch human resources, facilities and firm management. The days of cybersecurity simply being a matter of IT applying security patches are long gone.

or a data breach boils down to your preparation and plan, he adds.

"Cybersecurity is a process and should be part of the firm's other ongoing processes for conducting business," says Joseph Burton, Of Counsel at Duane Morris LLP in San Francisco, California, and Principal Consultant at Wescott Cyber Consulting. "It's really a risk management problem requiring input and oversight from management, and having a cybersecurity program that considers technology solutions, process solutions and administrative solutions."

The process-oriented approach contrasts what many firms have done in the past (or what some may be doing today).

"We call it the information supply chain. If you look at the flow of data — who touches it and has access to it — you need to follow that trail and verify that everyone is following the same best practices."

"Technical solutions are usually applied in an ad hoc, one-off manner without any thought as to how that fits into your overall security needs," Burton says.

While larger firms have the capacity to hire a full-time chief security officer or chief compliance officer, this may be too much for small and midsize firms. Burton suggests getting outside advice from a cybersecurity consultant or vendor who can assist your firm in meeting client requirements, answering questionnaires and completing on-site audits.

They can also help firms follow the information supply chain. INVISUS walks law firm clients through a risk management process that includes sending questionnaires to vendors. "Reputable cloud companies and document management software companies have been dealing with this for the last year or two," Harrison says. "They should be able to instantly reply with proof of compliance."

STEP BACK BEFORE STEPPING AHEAD

Over time, the requirements will only get more involved and complicated. Now is a good time for firms to take a step back and analyze cybersecurity from a management perspective. The trick is to know which standards to adhere to and to develop a process and a plan to ensure that your security measures are working.

With specialized expertise, legal management professionals can get ahead of the rising heat. Experts agree that it's important to find a vendor with law firm experience. They know your business, can drill down to requirements specific to your practice, and guide your firm into being an attractive partner for clients with regulatory and other cybersecurity needs. ■

ABOUT THE AUTHOR

Mark Brewer is a freelance writer who helps decision makers understand technology, trends and ideas to make them more effective in their work.

815-565-7272
mark@markbrewerwriter.com
markbrewerwriter.com