Legaltech news

Page printed from: *Legaltech News*

Experts to Firm Leaders: Cybersecurity is the Biggest Public and Private Sector Threat

As incidents abound, experts are still pushing for that cybersecurity wakeup call and are now pursuing the attention of the C-Suite.

Ian Lopez, Law Technology News

June 15, 2017

While major breaches may point to a wide array of targets for hackers, lawyers are high on the list of potential victims. As U.S. Department of Homeland Security assistant general counsel for cyber and infrastructure programs Gabriel Taran said of preferred targets, lawyers “are very popular, and that’s not a good thing.”

Taran and others across the private and public sectors addressed law firms’ current state of cyber affairs on June 15 at Thomson Reuters’ CFO/CIO/COO Forum. Their panel, titled “A Rumor of War: Regulation, Revelations & the State of Cybersecurity in 2017,” looked at what happens in a breach, how law firms have and should respond, and challenges to pushing forward with security initiatives.

Integral to an up-to-date cybersecurity approach is getting the attention of the C-suite, or partner in a law firm, level. Timothy Murphy, president at Thomson Reuters Special Services, said that CIOs and CFOs are necessary for bridging that gap.

“This is the most significant threat this country, businesses and law firms face,” said Murphy, who was previously deputy director of the FBI. Meanwhile, public policy remains “too slow,” while “public, private partnerships are still too narrow,” and the “tools and methodologies we use today are wholly outdated. We’re not on the cutting edge.”

Costs of a Breach

Hackers have various motivations and multiple actors, whether they be what Taran categorized as vandals, thieves, spies, saboteurs or bullies. While everyone is at risk with these actors, a law firm’s risk is compounded because they hold “data from every sector of the economy.”

And the costs of a breach are plenty. In addition to money, Taran points to “huge” reputational risk, loss of attorney-client privilege, and loss of trade secrets. This also opens up a host of potential legal issues, putting both law firms and general counsel in the hot seat.

Among potential questions firms may face are whether to call government entities and provide them with open access to company information, Murphy said.

Daniel Garrie, managing partner at consulting firm Law & Forensics, said that firms have to know what data has been leaked. But this presents a complex issue, as while firms have fiduciary responsibility to report instances to clients as well as regulators and government entities, their client can often sue.

This fact led into a discussion of what falls into the categories of reportable data and what a law firm may have not known was reportable data. Nicholas Barone, director and co-head of the cybersecurity practice at Eisner Amper, pointed to medical data as an example, which sometimes in itself may not legally qualify as reportable but often contains information that does qualify.

Murphy noted that if law firms are counting on federal and state legislation to help the issue, then they're not paying attention. "We all know it's hard enough to pass laws and regulations that make sense. … We cannot wait for them to pass policy."

"Policy is very slow. Law is even slower," Taran added. "It took Congress until 2015 to pass a law about sharing cybersecurity threat indicators and monitoring systems for cybersecurity threats. These seem like basic things that have been around since the '90s, at least."

Taran said that policy, "at the mental level, takes years to coalesce around, and there's a real problem with trying to catch up with technology. It's part of why we try not to regulate cyber, because that process in itself is a three to five year process. That would just make no sense and spit out something that would be obsolete."

What the Firm Can Do

While laws and guidance around response may lag, there are things firms can begin doing to better secure their data. James Quinn, head of security architecture at Infotecs Americas, suggested that one the first things to do is locating where data resides and classifying it. Then, the firm can adopt "layered defense"—protecting the most important information first and working downward.

Quinn added that when it comes to security updates, attorneys should do a "reverse Nancy Regan—just say yes."

To that end, Murphy said that if a law firm wants to mitigate risk right away at a somewhat moderate cost but high impact, taking steps like patching operating systems and applications, administrating control tightening, implementing two-factor authentication and encryption, and figuring out what data a company has to protect will mitigate about 80 to 90 percent of risk.

As for that additional 10 percent, Garrie noted that law firms probably won't be able to stop bad actors there, as firms lack the sort of budget utilized by major corporations like Chase.

"I think you need to embrace the reality that your firms operate in the culture that you're operating in," he added.

Taran said the government has information for law firms as well, such as cyber threat information shared by the Department of Homeland Security, the free assessment for vulnerability to spearphishing attacks and the like, and the FBI's partnership effort with the public sector, InfraGard. He also noted guidance provided by IT-ISAC and ISO/IEC 27001.

Murphy advised being aware of third parties' security policies, as this is where most breaches come from. Further, he said it's important to know that employee behavior is integral to security, as tools alone won't prevent breaches.

Organizations "put up tools, and we're still breached every single day," he said.

Contact the author at ilopez@alm.com.