Daily Labor Report®

July 12, 2017

Bloomberg BNA

Business of Law

Employment Lawyers Learn Cybersecurity Techniques

BNA Snapshot

- Some worklaw firms are training attorneys in cybersecurity
- Momentum for certification is growing

By Gayle Cinquegrani

Employment lawyers must learn to use technology wisely to reduce the threat of a cyberattack to their own data, especially those attorneys who may be advising their employer clients on safeguarding employees' personal information.

Lawyers make attractive targets for cyberattacks because "their files are a virtual treasure trove of information and data," John Reed Stark, a cybersecurity consultant in Bethesda, Md., told Bloomberg BNA July 10. "Lawyers are the guardians of corporate secrets."

A labor and employment firm may have client employees' health information and Social Security numbers, information related to clients' business strategy, and trade secrets from noncompete agreements.

The ever-present need for lawyers to remain vigilant to the threat of cyberattacks received heightened publicity recently when law firm DLA Piper was one of several companies hit June 27 by Petya, a global cyberevent that knocked out many of DLA's telephone and email systems. DLA Piper said it immediately began an investigation and remediation efforts and that no client data seems to have been breached.

Responsibility to Protect Client Data

The American Bar Association has recognized lawyers' responsibility to protect clients' data. The ABA's Standing Committee on Ethics and Professional Responsibility in May issued a formal opinion stating lawyers should undertake "reasonable efforts to prevent inadvertent or unauthorized access" to client information when they transmit it over the internet and "special security precautions" when required to do so by law, an agreement with the client, or the information's sensitive nature.

"Our lawyers have an obligation to protect our clients' data," and "our clients have begun asking" how the firm is handling that responsibility, Scott Shaw, FordHarrison's chief technology officer, told Bloomberg BNA July 7. To demonstrate its commitment to cybersafety, the management-side labor and employment law firm had all its legal professionals and staff certified in cybersecurity by the Legal Technology Core Competencies Certification Coalition (LTC4).

"Our firm was already aware of the risks and started a program to train our lawyers," Shaw said. FordHarrison had its lawyers go through LTC4's "Security for Lawyers" cybersecurity certification process because "it's important to have a measurable" sign of success, Shaw said.

LTC4 is a nonprofit organization established to create a standard skill set for legal professionals throughout the world, LTC4 contributing member Tony Gerdes told Bloomberg BNA July 6. Members—which could be law firms, corporate legal departments, law schools, or vendors—fund the coalition by paying fees based on their size. The coalition has members in the U.S., Canada, Australia, the U.K., and other European countries.

Certification Process

The certification process works like this: LTC4 provides the structure for the training and testing, while members provide the training or hire someone, such as an LTC4 vendor member, to provide it. “We set the standard and let the firm implement it as they see fit,” Gerdes said. Some of LTC4's vendor members produce LTC4-approved tests to assess core competencies.

FordHarrison bought the training content and assessment tool from an LTC4-aligned vendor and “tailored it to our needs,” Shaw said. “We tried to offer training in as many formats as possible,” including online and classroom training, email alerts, and a cybersecurity handbook. All 170 lawyers across all the firm's offices have been certified, and “we've incorporated the LTC4 certification into our new hire training,” Shaw said.

The move toward certifying lawyers’ expertise with technical skills is “gaining momentum,” and FordHarrison is beginning to note certifications on its web site, Shaw said. “There's definitely an expectation from clients that lawyers and staff will be proficient in using technology.” He said the firm has received inquiries from “client audits asking how we provide cybersecurity training to our lawyers.”

“The push for certifications has certainly grown over the last few years,” Gerdes told Bloomberg BNA in a July 7 email. Gerdes, the learning and development manager at Offit Kurman in Baltimore, predicted legal professionals will start listing their LTC4-certified skills on their resumes and LinkedIn profiles.

Formal Training Program

Constangy, Brooks, Smith & Prophete has a formal cybersecurity training program for its attorneys and staff but is not seeking to have them certified, the labor and employment law firm's chief information officer, Joe Ficocello, told Bloomberg BNA July 1.

The training, which is available online, was developed partly by the firm and partly by a vendor. Constangy's lawyers and staff “have to go through the training,” Ficocello said. “If we have noticed someone has recently lapsed, they will have to go through it again.”

Constangy's training tries to instill “good digital hygiene,” Ficocello said. It includes such practical tips as recognizing spam, ensuring “good password strength,” and refraining from posting personal information online that could be used to guess passwords. It also warns lawyers about leaving their smartphones unlocked and using hotel fax machines and file-sharing accounts such as Dropbox and Google Drive.

The training also encourages Constangy lawyers to use the more-secure Citrix software when working remotely instead of involving multiple devices by writing documents in less-secure software programs and emailing them from their personal account to their office computer. “People have to have good procedures in their personal life, too,” Ficocello said.

Carelessness Endangers Security

“The days that you can just install a tool to make your network secure are long gone,” cybersecurity consultant Stark said. “What's most important for cybersecurity is not the tools you have but the governance” of people's use of technology, he said.

Rushing or multitasking can cause lapses in lawyers’ cybersafety practices. They may accidentally send an email to the wrong recipient or leave a list of computer passwords out in the open or discuss confidential information over the phone in a public place.

The frenetic pace of lawyers’ work schedules makes it hard for law firms to monitor them, however. “There are so many ways you can do business. It's difficult for a law firm to control all those information lines,” which could include smartphones, laptops, home desktops, and computer tablets, Stark said. “Many lawyers pride themselves on being available to clients 24/7,” so “it's midnight and they just want to use the device they brought home” even if it isn't the most secure, he said.

In addition, lawyers who answer emails and calls after hours or while traveling are less likely to think about potential cyberthreats. “You're going to be responding when you're bleary-eyed and should be sleeping. That will make you more vulnerable to a phishing scheme,” Stark said.

“Good cyber is also good business,” Stark said, noting it can be a selling point with clients. “It's a good thing to market.”

To contact the reporter on this story: Gayle Cinquegrani in Washington at gcinquegrani@bna.com

To contact the editor responsible for this story: Tony Harris at tharris@bna.com