JUNE 14, 2018

Legaltech® news

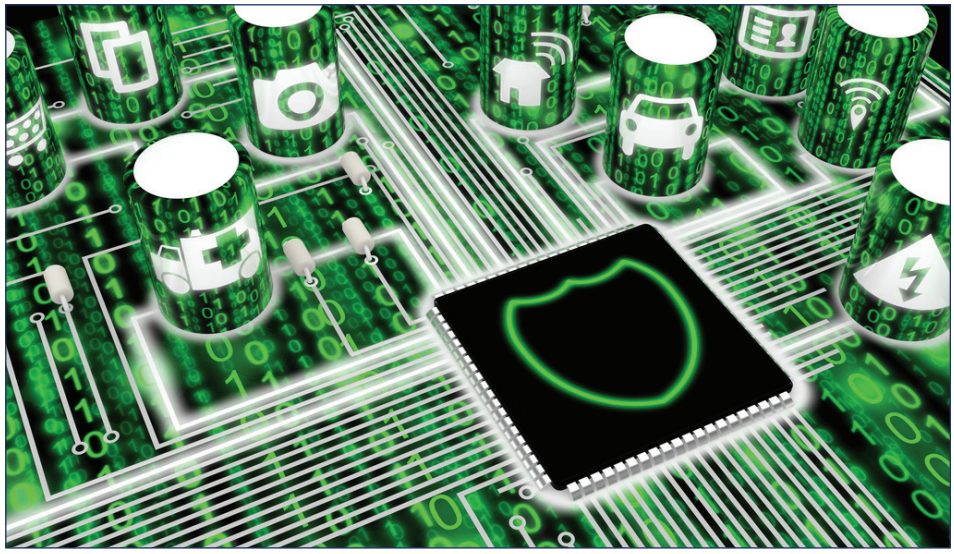
ONLINE

An ALM Publication

The Journey of Law Firm Security Assessments, From Genesis to Review

Legal ops professionals from Disney and Walgreens captured the changing law firm cybersecurity paradigm and some of the bumps they encountered in building evaluation programs.

BY ZACH WARREN



Back in early 2015, when Walgreens began implementing its outside security audits in earnest, the idea of ensuring third-party cybersecurity was still a nascent one. Oh, how much things can change in just three years.

These days, not only has the popular recognition and acceptance of cybersecurity as a worthwhile pursuit changed, but so too has the strategy necessary for corporate legal departments to review their outside law firms' security structure.

At the Association of Corporate Counsel Legal Operations Conference on Wednesday, in-house operations professionals from Walgreen Co. and Walt Disney Co., as well as an expert from Consilio, who has built many of these reviews for companies, captured the changing paradigm and some of the roadblocks they encountered in building these programs.

Karen Hornbeck, director at Consilio, started out by laying out four distinct ways corporations begin to make preparations: internal resources, external resources, third-party assessments and consultant-assisted preparation. In practice, many companies tackle the issue with a hybrid approach that combines these methods, but it was the internal approach that spurred both Walgreens and Disney when they built out their review systems in 2015 and 2016, respectively.

For Christopher Kopeck, senior manager of legal administration at Walgreens, the first step was to reach out to the company's internal IT security group—a relationship he continues to lean on heavily to this day. After a conversation, the ops team decided that they did not need outside assistance to develop a security questionnaire, only to bring together multiple parts of the internal organization.

"It was about synchronizing the effort between legal, our IT security group, our regular IT group, and our procurement, surprisingly," he explained. He later added, "We worked very closely with our IT security group. They're truly the experts in the space. … What's most important to our IT security group, and what should be most important to legal? We started there."

At Disney, the process was similar, building out a questionnaire internally. But then came the key question: Who actually should receive the questionnaire?

Tania Daniels, Disney's head of global legal operations, said that sending it out to every firm Disney worked with "was going to be a very long process with a lot of people to do it." Instead, the department decided to adopt a risk-based approach, filtering firms based on the volume of work and the type of information the firm receives.

The type of information piece is essential, the panelists said: It may require some information governance work to determine exactly what data is being sent where, but the time and security saved on the back end is crucial. Kopeck noted that Walgreens has both retail and medical elements, and firms that deal more with personal health information and labor issues were the first to receive the questionnaire.

"If we are in a government audit with Medicare or Medicaid, you're sending patient information. Those firms get scrutinized with a fine-tooth comb, because if that data gets out, it hurts us reputationally," he explained.

So you have a list of firms to send to and you have a questionnaire. How do you get the information to firms? Kopeck noted that Walgreens' strategy was to include security as an appendix of outside counsel guidelines, to ensure it gets followed. By putting it as part of the appendix rather than baked into the guidelines, the company is more easily able to update the security guidelines as needed.

"Every firm that agrees to work with us abides by the terms of that appendix, which was very helpful for us," he explained.

Hornbeck added that she had found it helpful if a general counsel or other executive specifically refers outside counsel to the security guidelines in a billing email or other notice, "A. to encourage participation, and B. to encourage honest answers." She relayed the story of one firm that had scored very well, until the corporation realized there had been a breach and the person filling out the assessment didn't have access to relevant information.

"Unfortunately, it can absolutely undermine the underlying trust of the relationship if you get answers back that aren't consistent with reality. … Here's the thing with breaches today: People are going to know. It's far better to be proactive and honest," she explained.

From there, it's a matter of following up. The panelists said audits can be a crucial part of the process (and should be included in the aforementioned outside counsel guidelines), but in practice should only happen with the most critical outside counsel partners, particularly ones that score poorly on the questionnaire.

Walgreens' IT security comes to the in-house lawyers with a stoplight approach: green for good, yellow for caution, and red for a problem. Disney's approach is more of a number score, spit out from the initial questionnaire and reviewed by IT. But either way, Kopeck said, if there is a critical concern, "We want to jump on that right away; we want to get information around that."

The most common mistakes Hornbeck sees are a lack of access controls, no subcontractor controls from the law firm end and incomplete or nonexistent incident response plans. For the latter, she added, "If you don't have a policy in place, you're not notifying anybody of anything within 72 hours. You're probably not even aware of it within 72 hours."

The panelists said that attorneys and firm relationship managers can be crucial allies in having the tough conversations. Daniels said that by keeping them in the loop, "they have ended up becoming the best advocate for requiring security from their firms." She noted that these attorneys can more easily get on the phone with other colleagues that use the firm, as well as partners. Kopeck added that he has even brought in his company's head of employment litigation and other key players into these calls to drive the point home.

Sound like a lot? It can be. Kopeck said that he originally thought the project would take two months—which turned out to be quite an underestimate.

Even though their programs have been ongoing for years now, both Kopeck and Daniels said they are still evolving.

But the effort is worth it, and law firms are beginning to see how crucial their own security is to the process.

"It's one of those things, it's not an unreasonable request anymore," Kopeck said, adding he'd encourage in-house counsel to reach out to firms "as often as you think you need to, and make them answer those questions."

Zach Warren *is the editor-in-chief of Legaltech News. He can be reached at zwarren@alm.com.*