

The Trouble With Implementing Cybersecurity Rules In BigLaw

By **Aebra Coe**

Law360, New York (May 9, 2017, 11:36 AM EDT) -- The Association of Corporate Counsel released cybersecurity standards in March aimed at increasing the data security of outside law firms, but there could be major complications to BigLaw's implementing the standards.

The guidelines are aimed at ensuring that sensitive client data remains confidential and are meant to serve as a benchmark for law firm cybersecurity practices, but some experts doubt firms' ability to meet the standards, at least in the near future.

According to Max Welsh, a senior risk management consultant for InOutsource, there has been an emphasis in recent years on efficiency and convenience, in terms of outside lawyers' practices, which has led law firms to allow them to access information almost anywhere, a policy he said is a potential problem for cybersecurity.

Firms have also been liberal with where lawyers can save information, which can make standards regarding information retrieval difficult, Welsh said.

There's a tension in law firms between client demands, an attempt to work efficiently, and keeping costs down, he explained.

"Law firms have had to try to meet the needs of a variety of lawyers that like to access information in different ways, at the same time responding to client desires that they buckle down on all the ways lawyers access the client's information," Welsh said.

Some of the policies and procedures laid out in the ACC guidance include the requirement that outside counsel have appropriate technical and organizational measures in place to prevent the misuse or loss of sensitive information, have adequate internal security and privacy policies in place, have incident and problem management procedures to mitigate and effectively respond to a data breach, and have adequate resources and management oversight to ensure cybersecurity policies are implemented.

The guidelines follow the release of ACC's 2017 Chief Legal Officers Survey, which found that two-thirds of chief legal officers and general counsel believe that information privacy and data breaches are "very" or "extremely" important.

The very structure of law firms can put them at a disadvantage when compared to the cybersecurity controls of the corporations they serve, according to cybersecurity consultant and author John Reed Stark.

"There's a cultural obstacle within," Stark said. "The partnership structure influences what law firms value and how much they'll pay people."

Money that is paid to a chief information security officer is money that comes directly out of partners' pockets, and Stark said the salaries being offered to CISOs at some law firms are a direct reflection of that. He said he heard of a law firm recently that was searching for a CISO and was offering to pay candidates the same salary as a second-year associate.

"And yet there is a huge demand for those people," Stark said. "You have to romance people in that space to get them hired. That means changing the entire approach to hiring. It has to be a much more thoughtful process."

Another way in which the culture of many law firms is in contention with cybersecurity, according to Stark, is in the day-to-day needs of lawyers in getting their jobs done.

In today's legal industry where competition is fierce, rainmakers are spending their time attempting to bring new business into their law firm and serving existing clients, many may not have the time or energy to make cybersecurity — which does not seem to be a profitable way to spend their time — their top priority, Stark said.

"It's very hard if you're a partner at a law firm and bringing in \$5 [million] to \$10 million a year in business and the administration tells you that you can't use the iPhone you want or laptop you want, or set up a home office the way you want it — that's going to create problems in that corporate structure. Law firms need to create a culture where cybersecurity is critical to everyone," he said.

That often means that law firm administration has to take a strong lead and create incentives for partners to comply, Stark suggested.

One major obstacle to law firm cybersecurity, according to Welsh, is information governance. Often, lawyers save information to multiple devices or in locations where it can be lost or forgotten.

When it comes to information governance, some law firms have "started down the road" of developing sophisticated systems, scaling back the variety of places lawyers are permitted to store information and instead pushing them to use official records repositories, Welsh said. But, "some are just getting started."

Those that can adhere to many or all of the ACC's standards can use that as a marketing tool to clients, Welsh suggested.

"That's a huge bonus, above and beyond the expertise of the lawyers," he said.

According to Joe Burton, a cybersecurity partner at Duane Morris LLP, there also may be complications implementing the new standards released by the ACC due to their rigid structure and seemingly contractual wording.

"[The standards] can be overreaching and intrusive, or could be perceived that way by law firms. I would expect that law firms might balk at or look askance at some of the issues in there because they get away from addressing security measures," Burton said.

For instance, the requirement that outside counsel will certify that it has returned all confidential information at the end of the matter "smacks of a liability-shifting effort" rather than an effort to simply improve security, he said.

Burton suggested clients and law firms can view the information from the ACC more as model concepts that they can consider including, rather than strict guidelines.

"I think trying to have standards is important and trying to move industries and individual law firms and individuals within those firms toward better security is a good thing. This is better than

nothing, which is what we've had for a long time," he said.

--Editing by Rebecca Flanagan and Emily Kokoll.

Correction: A previous version of this story misidentified Max Welsh's first name.