** Will print automatically! If it doesn't, click **here**. **

CRAIN'S
NEW YORK BUSINESS

Cybersecurity

Published: December 18, 2015 - 12:04 pm

Julia Brickell experienced a common challenge of keeping data secure when a client's vendor, a very well-regarded firm, agreed to her firm's written protocol on how to deliver information to her firm but promptly ignored it: "The first delivery, we got a hard drive with the password Scotch-taped to the hard drive," she said.

Brickell is executive managing director and general counsel of H5, a provider of eDiscovery and document review solutions for litigation and investigations based in Manhattan. She's not alone in her understanding that a corporation counsel can't assume that the best-laid data security plans will work in the real world.

"As chief legal officer, I have to make sure that employees are aware of every policy and procedure they are subject to," said Debbie K. Hoffman, head of legal, North America, for Mphasis, an HP company and the parent company of Digital Risk, LLC, in Manhattan. "They can't just be on paper. They have to be something the company understands."

High-profile data breaches are driving this heightened awareness among businesses. T-Mobile's data breach in September underlined for many the threat that companies face not just against their own database but also on that of outside partners with whom important data is shared. In the case of T-Mobile, hackers stole the personal information of 15 million customers off of a database at Experian Information Solutions Inc., a credit-reporting agency used by T-Mobile.

"If your customer data is in the hands of a third party, you have to make sure they are holding it securely," said Guido Gabriele, litigation supervisor at Grassi & Co., an accounting firm with three offices in the New York City metro area.

And there are no cookie-cutter solutions. "What's appropriate for Target may not be appropriate for the manufacturing facility," said James J. Giszczak, a member and vice chair of the litigation department at McDonald Hopkins, who focuses on data privacy and cybersecurity. His firm has turned to an outside provider, Great Bay Software, for cybersecurity support.

In this environment, corporation counsels are playing an increasing role in drafting policies to protect a firm's data, even when outside partners have access to it.

"Based on history, they are going to make vendors sign off on the fact they are in compliance," said cybersecurity expert Alan Berman, president and CEO of DRI (Disaster Recovery Institute) International, a nonprofit based in New York City.

Some attorneys are keeping a close eye on what is going on in banking, as they expect it will set the pace for cyber protections in other industries. On the national level, the Office of the Comptroller of Currency, in October 2013, issued a risk-management bulletin detailing expectations that banks practice effective risk management over activities performed both internally "or through a third party."

"The financial sector often leads the way," said Berman.

The onus is on attorneys to do their homework, given that the American Bar Association amended its ABA Model Rules of Professional Conduct in 2012, to include "the benefits and risks associated with relevant technology" as part of the requisite body of knowledge expected of lawyers to maintain competence. Said Brickell, "Cybersecurity risk is at the crossroads of law and technology."

CRAIN'S
NEW YORK BUSINESS
