Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Regulatory Risks Stunting Cyberthreat Info Sharing: Survey

By **Allison Grande**

Law360, New York (April 09, 2015, 9:53 PM ET) -- Financial institutions, health care providers and other companies in a broad range of industries are refraining from sharing cyberthreat information with the government due in large part to concerns about regulatory backlash, according to a survey released by Mayer Brown LLP on Wednesday.

Mayer Brown between November and February asked key executives and corporate counsel in 15 industry sectors — including finance, health care, professional services and energy — to answer a dozen questions about how their companies are preparing for and responding to cybersecurity incidents.

“Cybersecurity is an area of growing concern that affects our clients and many others in an increasing number of ways,” Mayer Brown partner Marcus Christian told Law360. “The general idea with this survey was to do something to gauge not only the kind of activities they are undertaking but also view the perceptions and problems they are facing.”

The survey asked respondents, on a scale of one to five, to what extent concerns about regulatory enforcement actions or other adverse regulator action impacted the company's willingness to share information with the federal government.

More than a quarter of the respondents chose three, the most popular response, indicating that the concern does factor into companies' information-sharing calculus. Only 14 percent said it had no impact, which was the second most popular answer.

“As a former federal prosecutor, and one of the things that I've found when dealing with clients and is reflected to a certain extent is this survey, is that there is a certain reluctance in engaging law enforcement and regulatory agencies,” Christian said. “The key concerns that people have are if they go to law enforcement, they may take over and the company will lose control or wind up with some sort of adverse action.”

Christian called the notion that a company could be prosecuted solely for being the victim of a hack “a myth.” But the fear was further illustrated by another survey question that asked participants if their company had built a close working relationship with a government entity on cybersecurity issues.

Forty-one percent of respondents answered no, while only 23 percent said that they had forged a bond with an industry regulator such as the Federal Trade Commissionand the Federal Communications Commission, 20 percent admitted to working closely with a law enforcement agency such as the FBI,

and 3 percent had close ties with a prosecutorial agency such as a state attorney general or the U.S. Department of Justice.

The issue of cybersecurity information sharing has heated up in recent years, with President Barack Obama, businesses, consumer groups and other stakeholders pushing Congress **to enact legislation** that would grant liability protections to companies that voluntarily share cyberthreat data with the federal government and each other.

However, Congress has failed to act, due in large part to disagreements over how to ensure that extraneous personal information is not being shared and over how far lawmakers should go to shield companies from liability.

While the Senate Intelligence Committee advanced a data-sharing bill last month, executives and corporate counsel who responded to the Mayer Brown survey held little hope that lawmakers would act anytime in the near future to ease their fears.

Although 84 percent of respondents said they expected clear national standards to emerge in the next five years on the topic of data breach notification — which is currently covered by a patchwork of 47 state laws — only 30 percent believed Congress would act within that time period to establish liability protections for information sharing.

In the absence of information-sharing protections, companies are increasingly looking for other ways to protect their systems, such as purchasing separate cyber insurance policies for liability, which 27 percent of respondents reported having. Some are also instituting the voluntary cybersecurity framework released by theNational Institute of Standards and Technology in February 2014, although nearly half of the survey respondents said they couldn't assess whether the fledgling framework has been helpful in managing cybersecurity risks.

“What we're going to see and what the survey shows to some extent is that companies are going to invest more time and attention as well as money in addressing cybersecurity risks and problems moving forward,” Christian said.

--Editing by Kat Laskowski.
