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

SEC's The New Sheriff In Town On Cybersecurity

By **Allison Grande**

Law360, New York (June 16, 2014, 4:51 PM ET) -- A U.S. Securities and Exchange commissioner's recent call for public companies to step up their monitoring of cybersecurity risks shows that the Federal Trade Commission is no longer the only cop on the privacy beat, revealing the SEC's intention to scour companies' cybersecurity measures and disclosures to ensure investors are in the know.

During a speech at a "Cyber Risk and the Boardroom" conference at the New York Stock Exchange on Tuesday, SEC Commissioner Luis Aguilar **urged public companies** to go beyond the impact to their bottom line in making data breach disclosures, and pushed boards of directors to play a more active role in assessing cyberthreats.

Both public and private companies are already feeling pressure from regulators — most notably the FTC, which has lodged more than 50 data-security enforcement actions — to make cybersecurity a priority. But for public companies, the commissioner's remarks provide a resounding reminder that they can't forget the SEC when making decisions about how to handle increasingly prevalent electronic information security threats, according to attorneys.

"The SEC is the new cop on the beat here," said Ed McNicholas, the co-leader of Sidley Austin LLP's privacy, data security and information law practice. "While the FTC is very much entrenched and isn't going anywhere, the SEC's interest in the area is a welcome addition. Its emergence signals that cybersecurity is not just a consumer privacy issue, but also a data security issue that could potentially be material to a company's operations."

The regulator first signaled its interest in 2011, when it issued staff-level guidance that pushed companies to disclose cyberthreats and incidents in their regulatory filings. The commission **stepped up pressure** in April by announcing its plan to conduct a series of examinations of broker-dealers in order to assess their readiness to prevent and respond to attacks on cybersecurity.

While neither action has resulted in formal enforcement proceedings, the tenor of the commissioner's comments Tuesday signal that public companies and data brokers may be getting their last warning to shore up their safeguards and disclosures.

"While the commissioner's remarks were remarkably consistent with what the SEC has been saying since at least 2011, there was more urgency," said Randy Sabett, the vice chair of Cooley LLP's privacy and data protection practice group. "The commissioner is stressing that this is a critical issue that companies can no longer just push off as a lower priority."

Since the SEC issued its disclosure guidance in 2011, companies have been grappling with exactly which cyberthreats and incidents need to be revealed in public filings to comply with their long-standing obligation to disclose information that could have a material impact on their bottom line. The result has been a **trend toward including more details** about potential threats and breaches in public filings, a pattern that attorneys expect to continue.

"It seems like [Aguilar] was making the comment that companies should err on the side of overdisclosing security incidents as opposed to underdiclosing them, which is not that surprising, considering that the SEC has been pushing for more disclosure in this area and will continue to do so," McNicholas said.

In determining how to craft public disclosures that don't leave out facts that the commission may view as pertinent, companies first and foremost need to make sure that they have a firm grasp on what security vulnerabilities exist and what impact the risks can have on the data that they hold, attorneys say.

"Companies want to pause and breathe deeply and see what they know and make sure that the information they send out is a fair and accurate disclosure of what the facts are, because they are going to be faulted if they're wrong about something as important as this," said Quarles & Brady LLP partner Joseph Masterson.

The importance of involving the board of directors in cybersecurity matters was driven home by Aguilar, who spent a large portion of his speech prodding boards of directors to put time and resources into ensuring that public companies are appropriately considering and addressing their cyber risks.

"The SEC commissioner's comments are clearly focused and potentially herald a new level of proactive board oversight over cyber risk and security at public companies," said Mark Schreiber, chair of the Edwards Wildman Palmer LLP's privacy and data protection steering committee and chair for privacy matters of the World Law Group. "Whether this is strong encouragement or prodding, it will likely become a reality, or at least best practice."

Aguilar recommended that boards look to a **voluntary cybersecurity framework** for critical infrastructure operators released by the National Institute of Standards and Technology in February to build the foundation of their assessment efforts.

"It has been suggested that the NIST cybersecurity framework could become a standard beyond [what] those companies considered critical infrastructure; this is a step in that direction," Dorsey & Whitney LLP partner Melissa Krasnow said.

Attorneys agreed that public companies would be wise to look to the framework — which outlines a set of cybersecurity standards and provides assessment tools to aid operators in implementing these safeguards in a way that is tailored to their business models — to inform their risk assessments.

"At the end of the day, it's really about [whether companies are] focused on managing the risks as well as they can, and the cybersecurity framework is certainly a helpful conceptual roadmap for the board to use in thinking about risk management," said Adam Golodner, the leader of Kaye Scholer LLP's global cybersecurity and privacy group.

If boards fail to use tools such as the cybersecurity framework to take stock of the data they hold and

the risks posed to it, the SEC appears more poised than ever before to step in, attorneys say.

“The SEC is not flexing its muscles yet, but they are certainly letting the industry know that this is an expectation for the future,” McNicholas said. “Companies need to take this seriously and develop response plans today, because if companies fail to do so, they can expect SEC enforcement actions.”

As evidenced by the fallout from recent breaches at Target Corp. and Wyndham Worldwide Corp., the possibility that directors can find themselves being named as defendants in shareholder derivative suits is also high, and the SEC's warnings will likely only serve to fuel investors' fire as well, attorneys added.

“Whether [the commissioner's] remarks will find their way to juries in these shareholder suits remains to be seen,” said Kenneth Rashbaum, the head of the privacy and cybersecurity practice at Barton LLP. “The remarks may appear to be inadmissible as evidence at first glance, but one should not underestimate the creativity of trial attorneys in these cases.”

--Editing by Elizabeth Bowen and Philip Shea.