Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

SEC Poised To Turn Cybersecurity Focus Into Enforcement

By **Carmen Germaine**

Law360, New York (July 7, 2017, 12:09 PM EDT) -- Officials at the U.S. Securities and Exchange Commission have made it crystal clear they're focused on how American markets and firms are preparing for and disclosing cyberattacks, and experts say public companies and regulated firms should brace for a wave of enforcement.

The SEC has been urging companies to bolster their cybersecurity for years now, making the area a priority on broker-dealer and investment adviser exams for three years in a row, and the agency's focus appears unlikely to change under new Chairman Jay Clayton.

Clayton said during his Senate confirmation hearing that he questioned whether public companies are adequately disclosing their cyber risks, and his picks to lead the SEC's enforcement division, Stephanie Avakian and Steve Peikin, said earlier this month that they believe cybercrime is the biggest threat to U.S. markets.

Paul Hastings LLP partner Robert Silvers, the former assistant secretary for cyber policy at the U.S. Department of Homeland Security, said the early indicators are that the new leadership team will take cybersecurity more seriously than ever — including cybersecurity enforcement.

"I think we've seen in recent years more enforcement with respect to cybersecurity and I think that's only going to escalate," Silvers said.

The SEC's attention to cybersecurity is nothing new. The agency's Office of Compliance Inspections and Examinations listed cybersecurity on its annual list of exam priorities in 2015, 2016 and 2017, and has implemented several sweeps to test firms' compliance and controls on cybersecurity.

The office also released a risk alert this spring after the WannaCry hacking attacks, warning broker-dealers and investment advisers to conduct regular penetration tests and vulnerability scans and implement system upgrades on a timely basis.

That alert also revealed that many firms aren't living up to the SEC's cybersecurity expectations. Of firms examined in a recent sweep, OCIE said, over a quarter of investment management firms didn't conduct periodic risk assessments of critical systems, and over half didn't conduct penetration tests to identify weaknesses and vulnerabilities in their

systems.

Ulmer & Berne LLP partner Frances Floriano Goins said that broker-dealers and investment advisers have been subject to stringent and particularized cybersecurity regulation by the SEC and broker-dealer watchdog the Financial Industry Regulatory Authority, and as a result cybersecurity violations by registered entities has been enforced more aggressively than those of public companies.

"The SEC and certainly FINRA, which regulates some of these entities, have not been particularly sympathetic" to hacked firms and regulated entities that aren't up to speed on their cyber protections, Goins said.

The SEC has already brought several enforcement actions against registered firms for cybersecurity failings, including fining Morgan Stanley Smith Barney LLC $1 million in June 2016 for failing to secure its internal client information systems and prevent a breach.

That case followed broker-dealer Craig Scott Capital LLC's $100,000 sanction over allegations it used non-firm email addresses to receive faxes, and investment adviser R.T. Jones Capital Equities Management Inc.'s $75,000 sanction for failing to implement proper cyber policies before a system hack.

On the public company side, the SEC published non-binding guidance in 2011 encouraging companies to disclose descriptions of the specific cybersecurity threats they face and the steps they are taking to mitigate those risks in their regulatory filings.

The agency has also already brought several enforcement actions against cyber criminals, including charges against a ring of traders who hacked into law firm websites to trade on confidential information about impending mergers and acquisitions, and a sting against a hacking ring that broke into news sites to trade on unpublished reports of transactions.

The SEC has yet to bring a case over public company disclosures of cybersecurity risks or data breaches, although one could be on the horizon, as the agency is currently investigating Yahoo over data breaches in 2014 and 2013 that exposed more than a billion accounts.

Agency officials have previously suggested they would bring enforcement actions in cases where an issuer was hacked.

Speaking in February at the SEC Speaks conference, Avakian said she didn't believe the enforcement division could "rule out" bringing a case finding an issuer liable under circumstances where the company knew it had vulnerabilities and failed to disclose that to the public. She added she could envision circumstances where the SEC would bring an action if a public company failed to disclose something they should have disclosed.

Silvers said that, while the SEC understands that regulated entities and public companies are victims if their systems are illegally breached, that likely won't bar an enforcement action. He noted the agency already frequently initiates an investigation after companies disclose breaches.

"It's early days, but I don't think firms are going to get a free pass on what the SEC views to be their cybersecurity responsibilities," Silvers said.

But John Reed Stark, the president of cybersecurity firm John Reed Stark Consulting LLC and former chief of the SEC's Office of Internet Enforcement, said it wasn't clear the agency would be willing under Clayton to bring a significant case against an issuer that fails to disclose its cyber risks.

"Stephanie Avakian has been very clear that cybersecurity has been a big priority for her in the enforcement division, but I do think that as the regimes change, the focus will be more on fraud," Stark said.

Avakian herself pointed out in her SEC Speaks remarks that the agency didn't bring cases against the law firms or news organizations that were hacked, saying it was the SEC's "view that the firms were the victims of the hacks."

Other agency officials have also questioned whether seeking large fines against public companies for various violations ultimately punishes shareholders. New Division of Enforcement Co-Director Peikin said it was "fair to question" whether corporate penalties achieve the intended results in an interview with Reuters.

Goins said Clayton may instead focus on making the guidelines for public companies' disclosure more stringent before authorizing enforcement over data breaches.

"The current SEC guidelines only talk about disclosure of risk, and so what they're really asking public companies to do is disclose whether there's a particularized risk of a cyber incident that's going to impact, in essence, the bottom line of the company," Goins said. "It's a somewhat limited guidance in terms of public company regulation."

Clayton singled out cybersecurity disclosures during his confirmation hearing, saying that while he couldn't comment on investigations into any particular breach, looking across the landscape of disclosure he questioned "whether the disclosure is where it should be."

He said he supported legislation that would require companies to disclose whether any board members have particular cybersecurity experience, and added he believed investors should know whether companies are thinking about cyber issues.

Stark said he expects that the SEC will eventually bring a case against a hacked company but will stick to an action involving egregious fraud where a company "was clearly exercising some deceit."

Preventing data breaches is akin to making sure your children never come home from school with a cold, Stark said — "an impossible task."

With that in mind, he said he expects the SEC to move away from the "broken windows" enforcement approach employed by former Chair Mary Jo White, characterized by enforcement actions against even small violations of market rules. Instead, Stark said Clayton's SEC will likely focus on how firms respond to a cyber incident, rather than whether the firm successfully prevented an incident in the first place.

As for regulated entities like broker-dealers and investment advisers, Stark said even if the SEC eases up on "parking violations," the agency will likely strengthen its exam program to ensure meaningful cybersecurity examinations.

"Firms should expect to receive robust and intricate deficiency letters with respect to their cybersecurity," Stark said.

Indeed, in early June SEC officials forecast that they intend to focus more on exams than enforcement. David Glockner, the regional director of the SEC's Chicago regional office, told an audience at the agency's Compliance Outreach Program that the agency has made a "conscious decision" to lead its cybersecurity efforts through the exam program rather than the enforcement division, according to media reports.

Looking forward, Silvers said that the SEC is still working out its cybersecurity requirements but that firms should know by now that the agency expects an organized cybersecurity program with tight access controls and serious incident response planning.

"With each new published enforcement action and published advisory, it becomes clearer what the SEC is expecting to see," Silvers said. "The SEC's made pretty clear by this point that they're going to be active in the space, so I don't think anyone can claim total surprise anymore."

--Editing by Emily Kokoll.

All Content © 2003-2017, Portfolio Media, Inc.