Blogs

Public companies confronting a cybersecurity attack should ready themselves for the arrival of a new party stepping into the breach—the U.S. Securities & Exchange Commission.

As several companies have learned, the SEC has recently opened enforcement investigations looking not only into whether several companies had adequately prepared for and responded to cybersecurity breaches, but also as to the sufficiency of their disclosures relating to the breaches. These investigations come on the heels of the SEC's April 2014 Risk Alert announcing that its Office of Compliance Inspections and Examinations ("OCIE") will be examining more than 50 registered broker-dealers and registered advisors, with a focus on cybersecurity. Given the SEC's enforcement activity, companies should consider preparing cybersecurity breach plan steps, including document preservation, the assembling of a legal response team (including privacy counsel and SEC counsel), and a review of any prior disclosures. In anticipating what the SEC might view as adequate

cybersecurity preparation, guidance may be found in OCIE's April 2014 Risk Alert. The sufficiency of disclosure issue implicates a key question—namely, what standard will the SEC be holding companies to? The SEC has taken a position in certain comment letters that are, at times, at odds with its own 2011 guidance, insofar as they push for disclosure of *any* cyberattack, regardless of materiality. This standard goes beyond the 2011 guidance, where the SEC stressed that disclosure depends on materiality and acknowledged that detailed disclosures could actually compromise a company's cybersecurity efforts.

Explore more in

White Collar & Investigations
Blog series

White Collar Briefly

Drawing from breaking news, ever changing government priorities, and significant judicial decisions, this blog from Perkins Coie's White Collar and Investigations group highlights key considerations and offers practical insights aimed to guide corporate stakeholders and counselors through an evolving regulatory environment.
Subscribe ?

View the blog