Davis Polk

Studies Reveal Companies Disclosing Cybersecurity Risks, to a Degree

September 9, 2013 | Client Update | 2-minute read

22% of the Fortune 501 to 1000 companies remain silent about their cybersecurity risks, compared to 12% of the larger Fortune 500 companies, according to a September **report** released by the Willis Group. Other than this key difference, the report found that the public disclosures by smaller companies were similar to the findings in the Willis Group's prior **study** published in June, which focused solely on the Fortune 500. In both cases, the primary risks identified included: loss or theft of confidential information, reputational harm, direct loss from malicious acts caused by hackers or viruses, and liability concerns from system breaches or failures. Only 1% of the entire Fortune 1000 disclosed any actual cyber incidents, which may be surprising given the number of press reports about breaches.

These public disclosures stem from the SEC **guidance** in October 2011 listing disclosure obligations that may require a discussion of cybersecurity risks and cyber incidents. Although the Willis Group reports found that a vast majority of companies stated that cyber-incidents would cause material or serious harm or otherwise adversely impact their businesses, the reports question whether companies provided the level of detail sought in the SEC guidance as to the extent of those risks.

The SEC wants information on the probability of future occurrences and their possible magnitude, including the potential costs and other consequences from the misappropriation or corruption of company data, as well as the costs of any preventative measures. According to the Fortune 500 report, more than half of the companies did not address the scope of the risk and none provided any estimated costs. Of the 11% of the Fortune 500 companies that complied with the SEC guidance to discuss cyber risks from outsourcing functions, many did not describe those functions or how they were handling the risks, as requested in the guidance. Almost half did not provide any information on protections against cyber risks, and companies that did respond referred to technical safeguards such as firewalls or intrusion detection, with only about 6% citing insurance coverage.

In May, Chair White issued a **letter** answering Senator Rockefeller's inquiry that the SEC expand public company disclosure regarding cybersecurity practices and risks. She noted that the Division of Corporation Finance had distributed over 50 comment letters focused on cybersecurity disclosure since 2012, and that she has asked the Staff to provide her with a briefing of the current disclosure practice, compliance with the guidance and further recommendations on company cybersecurity disclosure.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Ning Chiu
+1 212 450 4908
ning.chiu@davispolk.com
