CARLTON FIELDS

Investors Demand Cyber Security Transparency

March 05, 2013

Almost daily we hear about a new cyber threat or information security breach. Just last week one of the world's largest cloud services providers, Evernote, fell victim to an attack that resulted in a security breach that potentially compromised more than 50 million user accounts. As corporate America becomes better informed about the cyber threats facing U.S. companies, investors will demand more information and transparency about a company's information security policies and practices. A recent survey conducted by Zogby Analytics raises serious concerns for C-suite managers who are simultaneously facing increased scrutiny from regulators, increased demands from investors, and a need to remain mindful of the damage negative press can have on stock prices. According to the Zogby survey, 70 percent of investors are interested in reviewing company cyber security practices and almost 80 percent would likely not consider investing in a company with a negative history of attacks. Notably, the survey also found that 66 percent of investors said corporate responses to attacks are more noteworthy than the attacks themselves. Additionally, the survey revealed investors are twice as concerned if a company had a breach of customer data (57 percent) as opposed to a theft of intellectual property (29 percent). While consumer-related data breaches grab headlines, the findings on intellectual property theft are particularly alarming. They demonstrate a fundamental misunderstanding of the damage that billions of dollars' worth of intellectual property theft can have on a company's bottom line. U.S. lawmakers are trying to create comprehensive cyber security law. But whatever they pass will likely fail to completely address this complex and rapidly evolving problem. Additionally, large U.S. companies are starting to address cyber security issues in their annual reports. Goldman Sachs mentioned cyber security in its annual report on March 1, 2013, saying it has "developed and implemented a framework of principles, policies and technology to protect the information provided to us by our clients and that of the firm from cyber attacks." Carlton Fields has the expertise to help you prepare policies and purchase technology solutions to better secure your information systems. Additionally, we can help you create a privacy program that protects your clients and employees. If you have any questions regarding this alert, please feel free to contact us.

Authored By

Dennis J. Olle

Related Practices

Cybersecurity and Privacy