Akin®

Are You Another Target for Hackers? 2014 Cybersecurity Risk Disclosure Reminder

Jan 13, 2014

Reading Time : **3 min**

Recent incidents have highlighted just how relevant cybersecurity risks are to companies in the retail space. In December, Target Corporation announced that debit and credit card information for more than 40 million of its U.S. retail store customers was wrongfully accessed during the height of the holiday shopping season, a number that has since increased to as many as 110 million compromised accounts. Target had previously disclosed data security risks in its 2012 annual report. In its discussion of risk factors, Target said that "[t]he nature of our business involves the receipt and storage of personal information about our guests . . . If we experience a significant data security breach or fail to detect and appropriately respond to a significant data breach, we could be exposed to government enforcement actions and private litigation." Furthermore, Target disclosed that malicious attacks and security breaches could cause them to incur substantial costs and they could encounter a loss of guest confidence, which could adversely affect their results of operations. Target is apparently trying to mitigate these post-incident risks and potential damage to its reputation with consumers by staying out in front of the problem: publicly announcing the data breach, establishing a dedicated webpage for resources related to the breach, and offering free credit monitoring and identity theft protection to all Target customers. Earlier today, Target's CEO Gregg Steinhafel posted an open letter on Target's official blog offering an apology to customers and setting forth a numbered list of remedial steps the company is taking post-breach. Target is also using social media to interact with its affected customers; the company's official Facebook and Twitter feeds have been almost exclusively about the data breach since it was first publicly announced. Whether or not Target's risk factor disclosure is sufficient to ameliorate government action and private lawsuits and whether or not Target's handling of the breach can preserve its brand and reputation as well as manage the potentially substantial costs associated with the incident remain to be seen.

Another retailer, Neiman Marcus, confirmed on Friday that it was also subject to a data security breach in December. While not as robust as Target's, Neiman Marcus's most recent Form 10-K contained risk factor disclosure identifying cyber-attacks and breach of information security as significant risks to the company's operations. Neiman Marcus has apologized to its customers via Twitter, but so far provided few details of the attack as they continue to investigate. The U.S. Secret Service is also investigating the Neiman Marcus information breach, the extent of which is not yet known.

In light of these recent high-profile cyber-attacks, companies may want to take a fresh look at the SEC's 2011 Disclosure Guidance to determine if their current risk factor disclosures should be supplemented to identify risks as technology evolves and more incidents occur. Companies should also review their standard "forward looking statements" language to determine whether it could also use refreshing. In doing so, companies should consider whether or not cyber-attacks post a unique and material risk to their operations, and should discuss these risks in a way that avoids boilerplate language and statements of general risk applicable to all users of information technology. Although the disclosure should be tailored and company-specific and should provide enough information to allow investors to "appreciate the nature of the risks," companies need not provide potential cyber attackers with a "road map" of their security flaws or vulnerabilities, according to the SEC. And as Target's reaction to its data breach illustrates, disclosures may continue after a cyber incident, as the company continues to investigate and update affected parties and investors.

Categories

Capital Markets | Corporate Governance | Cybersecurity, Privacy & Data Protection