Bloomberg Law

Corporate Law & Accountability Report™

Cybersecurity

Corporate Cyber Risk Disclosures Jump Dramatically in 2017

More public companies described ''cybersecurity'' as a risk in their financial disclosures in the first half of 2017 than in all of 2016, suggesting that board and C-suite fears over data breaches may be escalating.

A Bloomberg BNA analysis found 436 companies cited ''cybersecurity'' as a risk factor in their Securities and Exchange Commission periodic filings in the first six months of 2017, compared to 403 companies in 2016 and 305 companies in 2015.

''Cybersecurity is no longer just an IT issue,'' Christopher Pierson, executive vice president, general counsel, and chief security officer at Orlando, Fla.-based business services provider Viewpost, told Bloomberg BNA. It is now an enterprise risk issue that ''touches upon every aspect of risk of a company.''

Companies list risk factors in their financial reports to help shareholders and potential investors understand the risks they face. While the disclosures can be vague or use generic language, they can signal to investors what a broad base of companies consider emerging risks.

Bloomberg BNA examined SEC annual and quarterly filings from 2010 to June 30 this year.

The increasing prevalence of corporate warnings about cyber threats also reflects that in this day and age, ''all businesses are data businesses,'' John Tomaszewski, a Houston-based senior counsel in the International Data Protection group at Seyfarth Shaw, told Bloomberg BNA.

''A lot of companies have realized that data is a capital asset and, as a consequence, they need to do disclosures on how that asset is managed,'' he said.

Data Breaches Data breaches can result in loss of sensitive corporate, employee or customer data, regulatory investigations, law enforcement action, and business-partner or consumer lawsuits. The decrease of stock price after a breach also can lead to shareholder class or derivative actions.

A 2017 Allianz survey found that risk managers and corporate insurance experts see cyber incidents as the second-highest business risk in the U.S., up 13 spots from 2013.

The survey also found that cyber incidents are the top emerging risk for the long-term future and the second-highest concern in the financial services industry.

Organizations are realizing that any data they collect can be breached or lost, Seattle-based Online Trust Alliance Executive Director Craig Spiezle told Bloomberg BNA. ''More and more companies are experiencing incidents'' with accidental loss or exposure of data, third-party breaches, or ransomware that ''can have a material impact to business and operations.''

FedEx Corp. said it could suffer a ''material'' financial impact after a June cyberattack affected the worldwide operations of its TNT Express delivery unit.

Among other high profile incidents, a 2013 data breach at Target affected 40 million credit and debit card accounts and cost the company $252 million through the end of 2014.

A 2014 attack on JPMorgan Chase & Co. compromised the financial and personal information of 76 million households and 7 million small businesses. That incident came after the company spent $250 million annually on cybersecurity.

Attacks are ''increasing in volume and velocity,'' Tomaszewski said. This gives attackers ''a lot more capacity to have a negative impact on the businesses that they attack.''

The move to cloud-based computing is adding to corporate angst over cybersecurity.

Cloud Computing The adoption of cloud-based technology in the last three years has meant a lot of businesses ''are doing some major transitional, transformational work in their IT infrastructures,'' Peter Tran, a Boston-based general manager and senior director in the Worldwide Advanced Cyber Defense Practice at RSA Security, told Bloomberg BNA. Companies feel they have less control over the cloud than they did hardware-based data centers, which may be leading more of them to list cybersecurity in their risk factors, he said.

The number of publicly available data breaches appears to be decreasing but media coverage of these attacks seems to be increasing, according to the Privacy Rights Clearinghouse.

Cyberattacks, like those targeting Anthem Inc., Sony Pictures Entertainment Inc., and Ashley Madison are ''front and center in mainstream, conservative business publications'' and generally have a ''higher level of visibility in the press,'' Tomaszewski said.

SEC Guidance Corporate disclosures of cyber incidents increased from eight in 2011 to 154 in 2012, likely as a result of SEC guidance in 2011 on when cyber incidents should be disclosed in financial filings.

The commission's guidance led to cybersecurity being ''elevated into the general counsel's office, into the board's agenda,'' Pierson said.

Pierson said that he expects to see boards start to add a cybersecurity expert. ''There's just too many items,

too many incidents, too many risks to not have a cybersecurity expert on major Fortune 500 boards,'' he said.

BY SHIRA STEIN

To contact the reporter on this story: Shira Stein in Washington at sstein@bna.com

To contact the editor responsible for this story: Yin Wilczek at ywilczek@bna.com

CARE ISSN 2330-6300