JPMorgan on Hackers

171 Pages - Source: Securities and Exchange Commission - Contributed by NYT News, The New York Times - Oct 08, 2014

In a regulatory filing in August, as the bank grappled with a breach, JPMorgan said its board and audit committee "are regularly apprised" of significant cybersecurity events.

A More Subtle Discloure of Hacking (p. 63)

Cybersecurity

The Firm devotes significant resources to maintain and regularly update its systems and processes that are designed to protect the security of the Firm's computer systems, software, networks and other technology assets against attempts by unauthorized parties to obtain secess to confidential information, destroy data, disrupt or degrade service, sabotage systems or cause other damage. The Firm and several other U.S. financial institutions continue to experience significant distributed denial-of-service attacks from technically sophisticated and well-resourced unauthorized parties which are intended to disrupt online banking services. The Firm is also regularly targeted by unauthorized parties using malicious code and viruses, and has also experienced other attempts to breach the security of the Firm's systems and data which, in certain instances, have resulted in unauthorized access to customer account data. The Firm has established, and continues to establish, defenses on an ongoing basis to mitigate these attacks, and these cyberattacks have not, to date, resulted in any material disruption to the Firm's operations or material harm to the Firm's customers, and have not had a material adverse effect on the Firm's results of operations. The Board of Directors and the Audit Committee are regularly apprised regarding the cybersecurity policies and practices of the Firm as well as of significant cybersecurity events.

JPMorgan Chase relayed new details of a hacking attack in October. Other disclosures have been more subtle. In a regulatory filing in August, as the bank grappled with the breach, JPMorgan said its board and audit committee "are regularly apprised" of significant cybersecurity events. That language did not appear in an earlier regulatory filing from 2013 or in an earlier quarterly report.