FAMILY WEALTH REPORT

Print this article

SEC Tightens Screws On Cyber-Breaches; How To Prepare For Increased Risk

Steven W Perlstein Beau D Barnes

13 November 2017

It looks as if US authorities, scarred no doubt by a number of high-profile cyber-security outrages, such as the breaches at credit score reporting firm Equifax, are going to take a tougher line in enforcing certain rules. Time will tell. In this article, Steve Perlstein, a trial lawyer at Kobre & Kim, and colleague Beau Barnes, consider what the SEC is doing and how industry professionals should prepare and reduce the risk of attacks and enduring damage to their business. This publication recently hosted a conference on cyber-security issues in Kobre & Kim's New York City offices. As ever, the editors of this news service are pleased to share these views with readers and invite responses. Readers can email tom.burroughes@wealthbriefing.com

A number of recent US Securities and Exchange Commission actions point toward more robust enforcement of cybersecurity rules in the coming year. Amid a year of high-profile cyber breaches, the agency has taken definitive steps to enable increased enforcement. Here are some recent actions, what they mean and actions you can take:

SEC leadership publicly foreshadows cyber enforcement. In April, the SEC's acting enforcement director noted that, although the SEC had not yet brought an enforcement action in the cybersecurity space, she could "absolutely" see the agency doing so.

SEC assessment finds persistent cybersecurity gaps. In August, the SEC released a summary of findings from its second major cybersecurity preparedness study of broker-dealers, investment advisers and investment companies. The agency found some improvements since its first assessment in 2014 but noted persistent gaps in firms' adherence to their written policies and procedures and inadequate system maintenance, such as use of outdated operating systems and failure to promptly install software patches. Notably, the report described the failure to quickly patch known problems as a "Regulation S-P-related issue," foreshadowing potential enforcement.

SEC creates Cyber Unit and begins related enforcement. In late September, the SEC announced the formation of an Enforcement Division unit dedicated to "cyber-related misconduct," including hacking of material nonpublic information, violations related to blockchain and distributed ledger technology, cyber intrusions, and threats to trading platforms and critical market infrastructure.

The Cyber Unit did not wait long to flex its muscles: Later that same week, it brought two separate blockchain-related enforcement actions focused on misleading and fraudulent statements in so-called initial coin offerings.

Each of these events is notable in its own right, but together they paint a picture of an agency on the cybersecurity offensive. Counsel for companies and individuals subject to SEC jurisdiction should be aware of the increased risk of enforcement actions related to cybersecurity and act to mitigate risks.

Here are a few steps that companies, investment advisers, and those who advise them can take to prepare for the new enforcement environment:

-- Assess your risk. A comprehensive independent assessment of your critical systems — including penetration testing and vulnerability scans — can provide invaluable insight into your cybersecurity strengths and weaknesses.

-- Fix easy problems. In its recent assessment, the SEC identified various steps that "nearly all" of the firms examined had undertaken, from preparing breach response plans to ensuring regular system maintenance. Cybersecurity isn't perfect security, but don't leave the low-hanging fruit.

-- Do what you say. Almost all firms have some written policies and procedures, but the SEC found that many such documents were overly general or did not reflect firms' actual practices.

-- Understand the risks. The SEC's posture makes enforcement likely but unpredictable, especially as it seeks a jurisdictional beachhead in new territory. Engage with experienced enforcement counsel to understand how your operations fit into the new risk environment.

-- Be prepared for a cyber breach. Understand your obligations, as well as your potential offensive remedies and options, should you have a breach. The more advance planning you do, the less chaotic the actual breach will be.

The authors

Steven W. Perlstein is a trial lawyer who focuses his practice on complex civil litigation related to commercial transactions, business breakup disputes and securities-related litigation. Mr Perlstein also litigates matters related to data security, particularly with regard to civil remedies available to prevent the widespread dissemination of proprietary information. In addition, Mr Perlstein often represents clients in white-collar criminal defense matters and regulatory investigations.

Beau D Barnes represents clients in government enforcement defense matters, internal investigations and regulatory actions. He also provides counsel on issues related to privacy, cybersecurity and fraud.