THE REVIEW OF
SECURITIES & COMMODITIES REGULATION
AN ANALYSIS OF CURRENT LAWS AND REGULATIONS AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 52 No. 5 March 6, 2019

THE EXPANDING ROLE OF LAWYERS IN ADDRESSING CYBER RISK AT FINANCIAL FIRMS

Cybersecurity regulatory compliance is imposing a myriad of new responsibilities on counsel of financial firms. The authors discuss, in detail, areas in which such counsel should play a key role, including "reasonable" cybersecurity protections, board oversight, public disclosures, and compliance with specific rules. They then turn to incident response, managing vendor risk, and M&A transactions.

By Avi Gesser, Matthew Kelly, and Samantha Pfotenhauer *

Over the last few years, cybersecurity has become everyone's problem. Major data breaches are costly, difficult to prevent, and cause substantial damage to a company's operations and public image. In 2016, a year in which at least 1,935 data breaches were reported, malicious cyber activity was estimated to have cost the U.S. economy between $57 billion and $109 billion.[1] Equifax alone spent $242.7 million in the seven months following its 2017 breach on related expenses.[2] Between 2013 and 2017, nearly $5.7 billion in losses were caused by a single form of cyber scam — the "business e-mail compromise."[3] For U.S. corporations — particularly those in the financial services industry — cybersecurity risks are not only operational challenges, they pose existential threats. As more companies and consumers fall victim to successful cyber attacks, pressure builds on regulators to act, which has resulted in a proliferation of cybersecurity regulations and guidelines. And with this increase in cyber regulation (as well as civil litigation) come important roles for in-house counsel in advising on data protection issues.

Not that long ago, cybersecurity was viewed as primarily a technical issue, to be handled by a company's IT department. But the rise of a robust regulatory framework means that government agencies

[1] THE COUNCIL OF ECONOMIC ADVISERS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 1, 20 (2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[2] Equifax Inc., Current Report (Form 8-K) (Apr. 25, 2018).

[3] SEC, REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934 REGARDING CERTAIN CYBER-RELATED FRAUDS PERPETRATED AGAINST PUBLIC COMPANIES AND RELATED INTERNAL ACCOUNTING CONTROLS REQUIREMENTS, Sec. Exch. Act Rel. No. 84429 at 1 (Oct. 16, 2018), https://www.sec.gov/litigation/investreport/34-84429.pdf.

* *AVI GESSER is a partner in Davis Polk's Litigation Department, representing clients in a wide range of cybersecurity issues and counseling companies that have experienced cyber events. He is a frequent writer and commentator on cybersecurity issues. MATTHEW A. KELLY is an associate in Davis Polk's Litigation Department. SAMANTHA PFOTENHAUER is a law clerk in Davis Polk's Litigation Department. Their email addresses are avi.gesser@davispolk.com, matthew.kelly@davispolk.com, and samantha.pfotenhauer@davispolk.com.*

INSIDE THIS ISSUE