Hughes Hubbard & Reed

Cybersecurity: 2016 Wrap Up

News & Events

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

Last year's news was dominated by a few highly publicized cybersecurity events. The year began with the FBI trying to hack into a terrorist's iPhone, resulting in a national furor over whether Apple should help the Bureau to do so. The presidential campaign brought endless squabbling over Hillary Clinton's use of a personal email server. And the year finished with President Obama imposing sanctions against Russia for hacking the Democratic National Committee and trying to influence the election.

While these events grabbed headlines, they had little actual impact on day-to-day business operations or cybersecurity law. From our perspective, the real story of 2016 occurred below the fold, where businesses continued to wrestle with large data breaches, the Supreme Court decided an important Article III standing case, and regulators increased their scrutiny of cybersecurity issues. We recap these and other significant events below.

Data Breaches Continued to Plague Businesses

There were a number of major data breaches in the commercial sector, including retail merchants and restaurant chains (Neiman Marcus, National Wholesale, Wendy's), hotel chains (Trump, Hard Rock, HEI), colleges and universities (University of Central Florida, UC Berkeley, Michigan State), and health care providers and hospitals (21st Century Oncology, Premier Healthcare, MedStar Health Inc.).

Internet service providers and social media sites were frequent targets. In 2016, Tumblr discovered that 65 million accounts had been compromised in its 2013 data breach. LinkedIn's 2012 data breach was also larger than feared, affecting up to 117 million accounts. MySpace discovered that its 2013 data breach had compromised 427 million accounts. The year ended with the largest data breach in history, when Yahoo announced that up to 1 billion customer accounts had been hacked.

Law firms were not immune. The breach of the Mossack Fonseca law firm resulted in the "Panama Papers" scandal, which implicated wealthy individuals and politicians from multiple countries. There were reports that Wall Street law firms, such as Cravath and Weil Gotshal, had been hacked. Last year also saw the first ever lawsuit filed against a law firm for failing to secure its client's data. *Shore v. Johnson & Bell*, Ltd., No. 1:16-cv-04363 (N.D. Ill. Apr. 15, 2016).

The near-constant reports of data breaches led to the tightening of corporate security measures and greater involvement of the C-suite. Businesses reviewed their response and recovery plans, made sure they had appropriate policies in place, and tested their potential vulnerabilities. Data breaches also affected deal-making, as acquiring companies began to focus more carefully on their cybersecurity due diligence. Indeed, Yahoo's data breach caused speculation that Verizon might seek a substantial discount off its $4.8 billion purchase price.

The U.S. Government Continued to be a Target

Businesses were not the only ones hacked. The U.S. government entered 2016 still reeling from the Office of Personnel Management data breach. In February, hackers breached the Department of Justice and released data relating to 30,000 Homeland Security and FBI employees. The IRS announced that its previous data breach was worse than it had thought. And Harold Martin, an NSA contractor, allegedly walked out the door of the agency with 50 terabytes of data, an amount that dwarfs the number of files stolen by Edward Snowden a few years earlier.

The Case Law Continued to Develop

In legal news, the Supreme Court decided *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), reaffirming that Article III standing requires both a concrete and particularized injury. Following Spokeo, a number of district courts dismissed data breach cases for lack of standing. See, e.g., Khan v. Children's Nat'l Health Sys., No. TDC-15-2125, 2016 WL 2946165 (D. Md. May 19, 2016); Kamal v. J. Crew Grp., Inc., No. 2:15-0190 (WJM), 2016 WL 6133827 (D.N.J. Oct. 20, 2016); Attias v. CareFirst, Inc., No. 15-cv-00882 (CRC), 2016 WL 4250232 (D.D.C. Aug. 10, 2016), appeal filed No. 16-7108 (D.C. Cir. Sep. 8, 2016). However, plaintiffs won an Article III standing case in the Sixth Circuit, setting up a split among the Circuit Courts of Appeal. Galaria v. Nationwide Mut. Ins. Co., Nos. 15-3386/3387, 2016 WL 4728027 (6th Cir. Sept. 12, 2016).

Connected Cars Worried Regulators

In March 2016, the National Highway Traffic Safety Administration ("NHTSA") warned that connected vehicles were increasingly vulnerable to outside hacks. In October 2016, NHTSA issued a guidance for the automotive industry entitled "Cybersecurity Best Practices for Modern Vehicles." The guidance calls for a layered approach to cybersecurity, maximizing protective measures and minimizing risk factors, such as "attack vectors." The Federal Trade Commission separately emphasized the importance of consumer privacy in regards to car GPS systems potentially collecting and storing driver location information.

The SEC Focused On Lax Cybersecurity

In June 2016, the Securities and Exchange Commission ("SEC") imposed a record-setting $1 million fine on Morgan Stanley Smith Barney LLC ("Morgan Stanley") for failing to safeguard client data. The SEC found that Morgan Stanley had failed to adopt written policies and procedures to protect sensitive information, which led to an employee downloading client information to a third-party server and eventually compromising 730,000 accounts. See *In re. Morgan Stanley Smith Barney LLC*, Exchange Act Release No. 4415, 2016 WL 3181325 (June 8, 2016).

States Increased Regulation

In September 2016, the State of New York announced a first-in-the-nation cybersecurity regulation, requiring financial institutions to maintain a comprehensive cybersecurity program. See 23 NYCRR 500. The State recently announced that it would relax some of the requirements and postpone the effective date of the regulation for two months to give financial institutions additional time to comply.

Regulation of Medical Devices

In December 2016, the Food and Drug Administration finalized a guidance addressing the cybersecurity of medical devices entitled "Postmarket Management of Cybersecurity in Medical Devices." The guidance recommends the locking of physical access to devices to avoid tampering, automatically timing out sessions after periods of non-activity, and establishing protections and procedures for updating devices.

Related People

Seth D. Rothman

Tyler Grove

Related Areas of Focus

Data Privacy & Cybersecurity