Despite Aversion to Regulation, Trump May Expand Cybersecurity Efforts

Skadden

01 / 30 / 17

This article is from Skadden's *2017 Insights*.

Contributing Partner

Stuart D. Levi
New York

Counsel

James S. Talbot
New York

Four Times Square
New York, NY 10036
212.735.3000

skadden.com

President Donald Trump's statements to date on regulation in general and cybersecurity regulation in particular suggest a conflict between his desire to strengthen the country's cybersecurity efforts and his general antipathy toward federal directives. Although President Trump may try to streamline and simplify the regulatory regime corporations face, he is unlikely to try to dramatically weaken U.S. laws in this area.

A Focus on Cyberdefense

Cybersecurity was a front-page issue throughout the 2016 presidential campaign, from Hillary Clinton's use of a private email server to accusations of hacking by the Russian government to general discussions regarding the country's cyberpreparedness in light of increasing threats from countries like Russia, China and North Korea. Although President Trump has challenged the intelligence community's conclusions as to the source and motive of the cyberattacks against the election process, he stated throughout the campaign that cybersecurity would be a priority for his administration. To that end, President Trump has announced the creation of a Cyber Review Team tasked with evaluating the country's cyberdefense and cyberoffense capabilities and created an elevated position — that of homeland security adviser, roughly on par with the national security adviser — for his top cybersecurity nominee, Thomas Bossert. In addition, Mike Pompeo, President Trump's pick for CIA director, has spoken on the importance of cybersecurity in the intelligence space. In some respects, these moves signal a focus on cybersecurity as a national security issue rather than as a cybercrime or commercial issue, but the president is likely to recognize that the two are inextricably interconnected.

Existing Trend Toward More Regulation Likely to Continue

More and more United States regulators have taken an active interest in cybersecurity issues, and the regulatory trend has been toward greater detail and specificity with respect to the requirements placed upon regulated entities. Starting in the late 1990s and continuing well into 2016, regulators took a broad, flexible approach to cybersecurity matters. They focused chiefly on self-evaluation and assessment of risk, with regulated entities determining for themselves the appropriate means to address risk. Regulators generally refrained from imposing specific security requirements.

In recent months, however, a number of state and federal regulators have signaled a desire for more specific requirements. In September 2016, the New York State Department of Financial Services (NYDFS) announced a regulation that will take effect in March 2017 and with which companies must comply by September 2017. It will place a number of specific requirements on financial institutions within its jurisdiction, including the use of encryption and multifactor authentication in certain circumstances, as well as specific staffing requirements. Similarly, in October 2016, the Federal Reserve, Office of the Comptroller of the Currency (OCC) and Federal Deposit Insurance Corporation issued a joint advance notice of proposed rulemaking (ANPR) outlining a sweeping set of cybersecurity requirements for the nation's largest banks. The notice described potential requirements for internal staffing and reporting channels in addition to overall risk management within institutions. The notice period for the ANPR closed on January 17, 2017, and the timing of next steps has not been announced.

The shift toward specificity in cybersecurity regulation appears to be driven by a number of trends, all of which are likely to continue in the near future. First, cybersecurity best practices are taking shape, so regulators have a better understanding of what steps are

necessary and reasonable to protect against cyberattacks. Second, existing regulation appears to have been inadequate to prevent successful cyberattacks, suggesting that companies need greater incentives to protect their systems. Finally, cybersecurity attacks continue to be front-page news, putting pressure on regulators to take action in their respective jurisdictions. Based on the foregoing, it seems unlikely that President Trump will instruct regulators to pull back on cybersecurity regulation.

In light of his professed aversion to regulation in general, however, President Trump may seek to streamline and harmonize federal regulations, perhaps by designating a single regulator as responsible for creating and enforcing cybersecurity requirements. Many have expressed concerns with the existing, multi-party regulatory regime — particularly the administrative burden of complying with different (even if complementary) technology requirements and the need to report to different regulators with overlapping jurisdiction. A financial institution, for example, might be subject to review by the Federal Trade Commission (FTC), the Securities and Exchange Commission, the OCC and the NYDFS, among others, each of which has issued guidance and/or requirements on cybersecurity matters. Designating a single cybersecurity regulator could alleviate these issues.

Possible Changes at the FTC

One area where President Trump could have a near-term impact on cybersecurity regulation and enforcement is at the FTC. As of his inauguration, two of the five commissioner seats at the FTC were vacant, and a third will become vacant on February 10, 2017, when current Chairwoman Edith Ramirez steps down. The ability to appoint the majority of FTC commissioners — as well as a new chair — provides the president with an opportunity to exert strong influence on the commission. (See "Antitrust Enforcement in the Trump Administration.") During the Obama administration, the FTC was the most active U.S. regulator when it came to bringing cybersecurity actions against companies. The FTC sought to penalize companies that did not fulfill their cybersecurity promises to consumers or otherwise provide adequate cybersecurity protection. Many asserted the FTC overstepped its authority in these actions, by adopting an overly broad reading of the "deceptive" and "unfair practices" prongs of Section 5 of the FTC Act.

Although we do not expect President Trump to curtail regulatory efforts to address cybersecurity issues overall, his appointees at the FTC may take a narrower view of the commission's authority. Under such a scenario, the commission could decide to take action only in the most egregious cases — such as where a company willfully misleads customers with respect to cybersecurity matters — without trying to establish a more general standard of cybersecurity "fairness" under the FTC Act. Such an approach would be consistent with an overall effort to streamline cybersecurity regulations in the United States, if the president decides to pursue such an approach.