2017: The Year of Big Shifts in Cybersecurity

Jonathan D. Klein, The Legal Intelligencer

May 30, 2017

There is rarely a day that goes by in recent months when the subject of cybersecurity and data privacy is not at the forefront of news stories. Whether related to hacking incidents during the presidential election, a breach at a major U.S. corporation (or two) affecting millions of customers, or the inadvertent divulging of government secrets, cybersecurity is the hot topic of the year. Yet, so often these news stories focus on specific incidents rather than the cybersecurity landscape in general and how it might be evolving as a result.

From the mid-1990s—when the concept of cybersecurity first started to develop with the advent of more sophisticated computer usage—to late 2016, the approach to cybersecurity regulation has routinely consisted of (with some exception) broad, flexible cyber guidance, initiatives or programs with little enforcement mechanisms or actual enforcement. Of course, some industries have always enjoyed more specific regulations (e.g., health care: Health Insurance Portability and Accountability Act of 1996 (HIPPAA), Health Information Technology for Economic and Clinical Health Act (HITECH); banks/financial services companies: Gramm-Leach-Bliley Act (GLBA)), but only in recent years has there been an increase in enforcement for failure to implement or follow certain cybersecurity protections.

In late 2016, for the first time, we saw a shift in the cybersecurity regulatory landscape from this broad, flexible approach to specific, enforceable requirements for cybersecurity and data privacy protection. As part of this shift, we saw states and companies taking matters into their own hands to increase cybersecurity efforts. So what is/are the cause(s) of this shift? There are many potential reasons for the shift (and cybersecurity practitioners and analysts likely have different theories for the shift), but here are some more commonly accepted bases.

First, the shift in cybersecurity regulations may be attributed to a general irritation at the continued inability of the federal government to pass specific cybersecurity regulations. Despite multiple attempts and even near successes, the gridlock of the federal government has consistently resulted in very little progress for cybersecurity protections. As most readers of this article know, passing legislation, particularly in these hyper partisan times, is a long and complicated process. Because of this lag time, if/when such cybersecurity legislation finally does make it to the final stages of the federal legislative process, such cybersecurity legislation may already be obsolete in context and time due to the rapid rate by which technology is evolving. Thus, federal gridlock has certainly contributed to the big shift.

Second, because of the lack of progress in the federal government related to cybersecurity regulation and the varying/inconsistent cybersecurity regulations in place, states and local

governments have become increasingly concerned about how to safeguard their governments and citizens from cyberattacks. This has had the unfortunate effect of creating a 50-state patchwork approach to more general cybersecurity regulations with each state wanting to craft its own laws. Indeed, in 2016 alone, 28 states considered cybersecurity legislation, 15 of which were successful and include provisions related to data security practices in government agencies, exemptions from state-related Freedom of Information Act and computer crimes. These state laws, however, are only the beginning of state-run cybersecurity regulations.

The passage of the New York Department of Financial Services' cybersecurity rules (the N.Y. Cyber Rules) applicable to banks, insurance companies and other financial services companies, 23 NYCRR Section 500, is a prime example of a state taking the lead on cybersecurity and representative of the big shift. The N.Y. Cyber Rules are very specific and even include mandates (with penalties) for companies to have a chief information security officer and for top level executives to review and certify compliance with the N.Y. Cyber Rules on an annual basis. As the federal government persists in its inability to draft and implement more specific - cybersecurity protections for certain industries, more states will likely follow New York's lead and the shift toward more specific cybersecurity regulations will undoubtedly continue.

Third, federal cybersecurity regulations in place to date have been varied and divergent in their application and framework and, recognizing this, federal agencies are starting to work together to create uniform approaches. In fact, in October 2016, the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) jointly published an advance notice of proposed rulemaking of "Enhanced Cyber Risk Management Standards" to strengthen protections in the financial services sector. Similarly, in January 2017, the National Institute of Standards of Technology (NIST) updated its Framework for Improving Critical Infrastructure Cybersecurity—the result of a collaborative process involving industry, academia and government agencies.

Fourth, after years of taking a passive approach to cybersecurity protections—potentially due to the theory that cybersecurity regulations would be implemented by the federal government or just general ignorance of the seriousness and effect of cyberthreats—it seems that companies are finally caring more about cybersecurity and how to respond to the ever increasing number of cyber threats. And for good reason are companies finally taking collective action: cyberattacks have become more of a "when" and less of an "if" in recent years with extremely detrimental and costly effects to a given company, its employees, and, most problematic, its customers. Because of this, companies are increasingly allocating resources to more sophisticated cybersecurity measures and working together to ensure these measures are effective and widespread.

For example, leading financial institutions came together in fall 2016 through the Financial Services Information Sharing and Analysis Center to launch the Financial Systemic Analysis and Resilience Center (FSARC), which will partner with the federal government to identify and mitigate risks in the financial services sector. FSARC represents what will likely be a trend of collaboration in cybersecurity with a goal of industry-specific standards for cybersecurity. It also

highlights an excellent illustration of the emerging public-private partnerships between private sector companies (with the resources to study and test effective cybersecurity measures without constitutional or statutory restrictions) and the federal government that will be critical to creating effective industry-specific strategic cybersecurity solutions.

A large question remains what the Trump administration will do to alleviate/worsen the cybersecurity regulation landscape and further aid/complicate the big shift already in progress. Given President Trump's outspoken desire for deregulation, more states may follow in New York's example to take on the responsibility of specific cybersecurity regulations. And yet, President Trump has indicated some intention to strengthen the country's cybersecurity efforts, even budgeting billions to increase cybersecurity-related spending in various federal agencies in his 2018 budget proposal. How President Trump hopes to continue to accomplish his competing desires to deregulate and strengthen cybersecurity regulation looms. Whatever the outcome, the big shift of 2017 in cybersecurity is likely to continue.

Jonathan D. Klein is an attorney at Clark Hill PLC in Philadelphia, Pennsylvania. He has extensive experience representing clients on a wide range of complex commercial litigation and on issues related to cybersecurity and data privacy. Jonathan's diverse practice includes, but is not limited to, financial services litigation, appellate work, and drafting cybersecurity incident response plans, counseling companies if/when a breach occurs, and developing/drafting valid and enforceable privacy policies and terms & conditions. Jonathan frequently speaks and writes on cybersecurity matters for legal and professional groups. Jonathan welcomes opinions about this article and can be contacted at jklein@clarkhill.com or 215.640.8535.