Advisory

FEBRUARY 2014

Cybersecurity Legislation: Is Congress Ready?

Congress grappled last week with the merits and costs of several new cybersecurity proposals, each designed to protect consumers and stem the tide of recent data breaches that have engulfed U.S. businesses. Whether this activity will result in new law remains uncertain; nevertheless, the debate on federal cybersecurity governance likely will lead to changes in how U.S. consumers and companies conduct business.

Congressional desire to pass cybersecurity legislation has been motivated in part by the growing cost of data breaches to American businesses. According to the Ponemon Institute, in 2012 an average data breach cost a U.S. company over $5 million. Recent events illustrate that for large companies experiencing a significant data breach the loss will be much greater. In fact, some analysts estimate Target Corp.'s recent data breach may end up costing the company between $400 million and $1 billion. Of course, a loss of even several hundred thousand dollars may be catastrophic to smaller businesses, which are no less vulnerable than larger firms.

Congress also has been motivated by the harm recent breaches have inflicted on tens of millions of American consumers. These consumers, who initially were shocked to learn their virtual identities (including names, e-mail and home addresses, and credit and debit card and telephone numbers) were lost in the breaches, are now learning that their information is being bought and sold on websites that function like shopping malls for criminals.

Recent congressional activity is attempting to address these issues in several ways. Some of the proposals seek to compel U.S. businesses to adopt the "chip-and-PIN" credit card security measures used in Europe. Proponents point out that such a system would add a substantial amount of security for consumers making credit card purchases and reduce the probability of a Target-like breach. Opponents argue that scrapping the existing U.S. credit card system in favor of the chip-and-PIN system would cost billions and take years to implement. Other proposals call for legislating minimum corporate cybersecurity measures similar to the voluntary standards contained in the Cybersecurity Framework that the National Institute of Standards and Technology will release this week. While such proposals could boost security by putting in place minimum data security standards, these measures may be difficult to pass in the current political environment. There is a source of general agreement across the proposals, however. Most of the proposals call for creation of a federal data breach notification standard. Compared to suggestions to overhaul the credit card system or to mandate specific cybersecurity standards, a national breach notification standard is easier to implement and is more likely to have bi-partisan support. Passage of such legislation would have important implications for consumers and businesses.

CONTINUED ON NEXT PAGE

If you have any questions about this Advisory, please contact:

DAVID HALL
215.988.8325
dhall@wiggin.com

JOHN KENNEDY
203.363.7640
jkennedy@wiggin.com

MICHAEL MCGINLEY
203.363.7638
mmcginley@wiggin.com

Cybersecurity Legislation: Is Congress Ready? CONTINUED

A national data breach notification standard could supplant the existing, state-level data breach notification laws (currently enacted by forty-six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands) that have created a costly headache for companies attempting to comply with them. The patchwork of state notification requirements is messy and sometimes contradictory—particularly when breached records include personal information from a customer base spanning multiple states. Companies, for example, might be required to notify customers in one state that their data has been compromised and yet have no legal requirement to inform similarly situated customers in adjoining states.

Congress has been unsuccessful in several previous attempts to create a national breach notification law, so hopes that an agreement will be reached this term are measured. Yet the vigor with which Congress is now pursuing such a law is noteworthy. Within the past month, four senators—Richard Blumenthal (D-CT), Tom Carper (D-DE), Jay Rockefeller (D-WV), and Patrick Leahy (D-VT)—have advanced bills that include a federal data breach notification standard. For example, on February 4 Blumenthal introduced a bill that would require businesses to notify customers "without unreasonable delay" in the event of a breach. Leahy's bill also would require notification to be made without unreasonable delay, while Carper's bill would allow federal agencies to determine the time period within which notification must be made. Rockefeller's bill takes a slightly different approach and would require notification within 30 days.

At a Senate Judiciary Committee hearing on February 4, Leahy said that data security and privacy deserves bi-partisan backing. He noted that "most Americans, myself included, have been alarmed by the recent data breaches," and asked for support of his proposal to create a national standard for businesses to notify consumers of data breaches. Senator Chuck Grassley (R-IA), sounded a similar note at the hearing, commenting that "[t]here's widespread support for a national breach notification standard" and suggesting that Congress should focus on passing a breach notification law before attempting to tackle other data security issues.

Calls for a federal notification standard also have appeared in the House. On February 5, Representative Lee Terry (R-NE), stated his intention to introduce his own breach requirement legislation "that would foster quicker notification by replacing the multiple—and sometimes conflicting—state notification regimes with a single, uniform Federal breach notification regime."

Federal enforcement agencies also are supporting the idea of a consolidated federal notification standard. In congressional testimony last week, Jessica Rich, Federal Trade Commission ("FTC") Director of the Bureau of Consumer Protection, stated that the FTC has "long supported" data security legislation that would create a federal data breach notification requirement. In separate testimony, Acting Department of Justice Assistant Attorney General for the Criminal Division Mythili Raman called for a "strong, uniform Federal standard requiring certain types of businesses to report data breaches and thefts of electronic personally identifiable information." Raman also cautioned that not all breaches would require notification, and that the government should provide a "safe harbor" if a data breach has "no reasonable risk of harm or fraud."

Given the track record of the current Congress, it would be unwise to assume that even a shared desire by both legislative parties and the executive will yield any type of cybersecurity legislation, even a breach notification law. Yet it seems that every day Americans are hit with a new reason to worry that their personal information has been compromised, and this collective concern very well could be the impetus Congress needs to act.