Five Cyber Security Takeaways From the Mid-Term Elections

This article was originally published on The Huffington Post on November 12, 2014.

by Brian E. Finch

Brian E. Finch
Public Practices
+1.202.663.8062
brian.finch@pillsburylaw.com

Brian E. Finch is a partner in Pillsbury's Public Policy practice in Washington, DC. He is a recognized authority on global security matters and is co-leader of the firm's Global Security practice.

While not a much-discussed topic during campaign season, federal policy on cyber-security will likely see some material changes as a result of a Republican-controlled Senate. Just how significant those changes will be has yet to be determined, but here are some thoughts on probable outcomes:

1) Don't expect comprehensive cyber security legislation just yet: No matter what number of Senate seats wind up going Republican, one things is for sure - they will not reach a veto-proof majority. Without that, there is essentially no chance for a cyber security bill that will set a federal standard for security measures. Such legislation has been tried several times before, and the fundamental fact remains that the Senate is still divided between pro regulation and pro positive incentive factions. Given the rules of that Chamber, there is little chance that a bill establishing a baseline for security measures will pass anytime soon. Expect instead "small ball," whereby smaller bills with limited purpose and effect will be advanced, perhaps even passed into law.

2) The rhetoric against foreign governments conducting cyber-attacks will heat up: Members in the House and Senate have not historically been shy about pointing fingers at foreign countries that conduct cyber-attacks. However, the intensity of those attacks will likely rise in the new Congress. This is for a variety of reasons, starting with the fact that you now have a crop of younger, technologically sophisticated Congressional freshmen. There will be owners of cloud computing companies, military veterans, and former undercover officers in the Republican ranks now. They and others grasp the fact that other countries are plundering our national treasure through digital means, and more needs to be done to stop that behavior. Pointed floor speeches, demands to Cabinet Secretaries, and even punitive language tacked on to "must pass" legislation should be coming our way soon.

3) Executive policy will roll along, albeit with slightly more input from Congress: President Obama has made it clear that cyber security is a top priority in the Executive branch. His Executive Order 13636 resulted in the creation of a cyber "framework" as well as a reexamination of federal procurement policy. A more recent directive is pushing the Federal government to only use payment cards with "chip and pin" technology. This trend will not slow down at all. Numerous Federal agencies are increasing demands on their contractors to do more to protect their own systems as well as the

ones they service on behalf of the government, and the consequences for failing to do so will be increasingly severe. Congress may push back at times if there is a sense of "overreach," but in reality the president will likely push ahead on increasing cyber security via policy decisions.

4) The privacy versus security debate will live on: The Senate in particular lost some very staunch privacy advocates, chief among them Colorado Senator Mark Udall. Despite these losses, there are many forceful privacy advocates remaining in both legislative chambers, and they will not go quietly into the night. Mr. Snowden is still roaming free, and more revelations from him should be expected in the coming years. The net result of that will be continued battles over whether the Federal government is infringing upon the privacy rights of Americans as it monitors electronic communications. Of course, lost in that debate will be the subtle but critical point that when we are talking about cyber security, monitoring for malware really doesn't raise privacy issues. That's a shame, because the government itself needs to do more to detect, deter, and defeat cyber-attacks. Right now it isn't doing enough, and for sure the private sector is outgunned and outmanned.

5) All bets are off if a serious attack happens: We have had about as many serious data breaches as one could imagine in the past few years. It seems as if a majority of the population has had its credit card or personal information stolen at some point. Yet this has been met with a collective yawn in terms of actual legislation out of Congress. Sure there have been hearings and the verbal flaying of executives, but there is nary a sign of a universal data breach legislation on the horizon. All bets are off, however, if the country suffers a real and serious cyber-attack, I'm talking about financial markets being knocked offline, utilities going out, or a major business (or businesses) going under as a result of a cyber-attack. Should that happen - lookout. Congress will respond fast, and fast is not necessarily a good thing. Hurried legislation is often riddled with holes, and I would not expect a cyber security bill expedited into law as a result of a massive cyber-attack to be any different.

At the end of the day, one thing is absolutely sure - the cyber problem will not go away. So it will always be on the Congressional agenda in some fashion, with the only question being how high it rises.

Pillsbury Winthrop Shaw Pittman LLP | 1540 Broadway | New York, NY 10036 | +1.877.323.4171