Companies Facing Cyberattacks From Nation-States Need Better Legal Protection

This article was originally published by the *Wall Street Journal's* CIO Journal on June 22, 2015.

by Brian E. Finch

Brian E. Finch
Public Policy
+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.

Furious. Incensed. Appalled. Those are just a few of the less colorful adjectives being used to describe Washington's reaction to the ever-expanding hack of the U.S. Office of Personnel Management. "Fuming" has been used so many times it's a wonder that smoke alarms are not constantly blaring on Capitol Hill.

No doubt the autopsy results from this cyberattack will be especially ugly. Should this hack also prove to be the handiwork of the Chinese government, it will add more than a little insult to injury. Indeed, it may well finally force Congress and the White House to confront the fact that nation-state cyberattacks are essentially unstoppable.

And that may well be the most important lesson learned from this fiasco: if the U.S. government cannot stop a foreign government from stealing personal records, why should private companies be expected to do so?

That reality can and should have a material impact on how Congress approaches cybersecurity legislation going forward. With some careful drafting, there is a way for Congress to create a legislative silver lining to this gloomy event.

Congress should use the OPM cyberattack as a justification to limit the private sector's legal responsibility when it suffers a cyberattack from a foreign power or its cronies. Doing so will not take a heavy legislative lift—in fact a few simple tweaks to any number of bills already in the Congressional hopper will do the trick.

Congress should pick any given bill that calls for a uniform federal data breach notification standard and add on three relatively minor features:

First, Congress should suspend all government imposed data breach penalties if investigations prove a connection toforeign nation-state or a hacker group it sponsors or condones.

The suspension of those penalties is justified by the aforementioned reality that no private company can stop a foreign nation-state's cyberattack. As a matter of public policy Congress should not allow companies to be financially penalized for simply being the victim of such an attack. Moreover this penalty suspension should apply to both state and federal laws, particularly since state data breach laws are the largest source of heartburn for companies.

Second, Congress should continue to allow tort claims against private companies following a foreign government or foreign-sponsored cyberattack, but it should raise the bar needed to succeed in such suits.

Here, Congress should entitle private companies to have tort lawsuits dismissed when the breach was committed by a foreign power. However, courts should be able to reject that dismissal if the private company committed fraud, willful misconduct, or gross negligence when implementing their cybersecurity programs. That balanced approach should be enough to keep companies committed to maintaining a robust cyber security program.

Third,the U.S. government should help define which hackers trigger the aforementioned protections by establishing a list of state-sponsored or aligned hacker groups.

This list, which could be maintained by the Department of Homeland Security, State Department, or any number of other cabinet agencies, would represent the "master" list of organizations that, if shown to have committed a cyberattack, would trigger the penalty suspensions or tort limitations. Given the incredible proliferation of hackers, private companies could also petition the responsible agency to have the group that committed a particular cyberattack added to this list.

Protecting Americans from enemies foreign or domestic represents the most fundamental obligation of the U.S. government. In today's world, that obligation extends to the digital domain, not just the physical world. Penalizing American businesses for having been attacked by foreign powers is entirely antithetical to that basic mission, and so Congress and the President should step up and change the law to avoid that perverse outcome. Given its relative lack of success in fighting our cyber battles, making these small legislative changes is the least it can do for its citizens.