What Do I Need to Know and When Do I Need to Know It?

This article was originally published in the *Huffington Post* on August 14, 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 Washington, DC office. His practice focuses on counseling on regulatory and government affairs issues involving the Department of Homeland Security, Congress, the Department of Defense, and other federal agencies.

Another day, another big hack discovered. According to reports from the *New York Times*, the *Wall Street Journal*, and numerous other publications, a small group of cyber criminals based out of Russia were apparently able to collect around 1.2 billion usernames and passwords from more than 400,000 websites globally. The company that identified the hack, Hold Security, estimates that this hack is impacts more than 500 million people. Think about it: nearly one in ten people worldwide were apparently impacted by this attack. If true, wow.

Hold Security also—at least initially—said that for a fee it would provide website operators with information that would enable them to determine whether they were breached and would assist with future ongoing threat monitoring.

I won't go into the merits of the decision of Hold Security to charge for the information it has collected ... that's a discussion for another day. But it does raise an interesting series of questions about what one should do if it comes across evidence showing a website breach or if a company has an obligation to track down this kind of information.

This type of situation is typically much cleaner when the entity retaining the information about the breach is a law enforcement agency. Odds are officials will notify you of the breach, even if they will not share details of how they learned of the attack or when. Congress is also trying to make this kind of scenario less complicated by allowing for increased information sharing between the public and private sector. Of course that effort is stymied in large part due to concerns about protecting the privacy of individuals (thank you very much Mr. Snowden).

For me, the most interesting questions though relate to what a business owner should do in this kind of situation. Do they pay up to the security vendor to find out whether their digital house has been broken in to? Are they obligated to do so under any kind of express or implied obligation? Or perhaps they follow the old Sgt. Schultz defense ("I see no-zing, NO-ZING!!"). And if they do pay the "security fee," can they seek reimbursement from insurance carriers for the money spent, much less the money spent to identify and fix the vulnerability as well as any associated damages.

I am not sure where this is going to go, but it is certainly a thread worth following. Most would agree that cyber intrusions are only becoming more numerous, and so companie—and in particular their directors and officers—are going to have to confront these kinds of issues sooner or later. I would note that there are certainly are plenty of tools already available that can help detect these kinds of attacks (automated information sharing, continuous monitoring, etc.), but the cost of those tools may not be within every company's budget.

Still, the fundamental question remains; how far does a company have to go to find out whether it has suffered a breach? Some sort of line has to be set, if for no reason other than letting companies know what they should do every time someone says "Hey, pssst, buddy, pay me $50 and I'll tell you if you were hacked today."

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