Defending Data Post-Anthem

This article was originally published on Huffington Post on February 12, 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.

Companies, especially health care providers and insurers, should take measures to prepare for further cyber attacks.

Given the number of high profile data breaches in the past 18 months, it should have come as no surprise that Anthem Insurance Companies recently suffered a massive loss of customer information. Details are still being gathered about the amount of information lost, but there is near certainty that the Anthem attack will be one of the biggest in history (so far).

What is particularly worrisome about the Anthem data breach is the apparent source of the attack along with the methods used. Industry experts have preliminarily laid blame for the attack at the **feet of Chinese hackers**. Moreover, all indications are that the attack was extremely sophisticated, using advanced malware that would breach the most commonly used cyber defenses as well as more sophisticated defensive measures.

The Anthem breach fits well into a recent pattern of foreign governments or their agents breaking into health care companies, insurers and other organizations storing vast amounts of personally identifiable data such as names, home addresses, social security numbers and other unique bits of information.

The motivation for these attacks is unclear, but speculation centers on enabling medical fraud or, more likely, using the personal identifiers to commit new and hyper-targeted attacks intended to penetrate into sensitive corporate and government networks.

Unfortunately, there is no sign that Anthem-like attacks will slow down, and so companies should proactively take steps to ensure that they are as prepared as possible for a similar event.

To that end, we offer the following suggestions on how health care providers, insurers and others in the health care industry can boost their cyber-preparedness:

- **Connect with the National Health Information Sharing and Analysis Center:** The National Health Information Sharing and Analysis Center (NH-ISAC) is a not-for-profit organization dedicated to sharing physical and cyber threat information amongst members of the health care community. NH-ISAC professionals and members can help health care companies learn more about the Anthem attack, including indicators of compromise (IoC) to monitor for. Having such IoCs can be extremely helpful in determining whether your company is being monitored for actually under cyber attack.

- **Immediately Conduct a Review of Your Information Technology Systems For Signs of Compromise:** The Anthem attack is one in a series of attacks on health care and other companies holding tremendous amounts of personally identifiable information. Every company should consider itself at risk for such an attack and, to be blunt, should not be surprised if it has, in fact, been hit by such an attack. Health care companies should therefore proactively reach out to their cyber security providers and ask for an immediate sweep of their systems for signs of attack or data loss. Ideally, companies would be continually monitoring for such events, but the sophistication of the Anthem attack suggests the need for a "deep-dive" cyber forensic investigation.
- **Use This Incident as an Opportunity For a "Data Diet":** One interesting tidbit that has emerged from the Anthem attack is that apparently some of the information stolen belonged to people who were no longer Anthem customers. This so-called "zombie data" poses a serious risk to companies, because its retention only broadens its exposure should a cyber attack occur. Companies should therefore use this opportunity to review its data retention policies, and where appropriate seek to delete/destroy data that is not needed, much less required to be retained. Doing so will decrease the amount of records that can potentially be lost, and it also will allow security professionals to focus their resources on truly valuable information.
- **Review the Security Posture of Business Partners:** While not necessarily the case in the Anthem breach, many times successful cyber-attacks originate from business partners whose security has been compromised. Health care companies should review the defensive posture and contractual agreements with their business partners, information technology vendors and any other organization that has access to its digital systems. Take this opportunity to see exactly what obligations -- if any -- such partners have to secure transmissions or information as it is being shared. Cyber attacks can come from any number of directions, and so companies are better off if they take the time to ensure that their business partners are taking appropriate defensive measures.
- **Assume that a Breach Will Occur:** This is a piece of advice that is a bit hard to swallow, but is also absolutely necessary. Health care companies should assume that they will at some point suffer a similar breach. The sophistication and innovation of cyber attackers essentially guarantees that outcome. Accordingly, companies need to review their incident response plans in order to ensure that the plans are up to date and adequate for a potentially massive data breach. Appropriate response plans will include knowing who will manage the response to the breach, as well as having agreements in place with counsel, crisis communications firms, outside security vendors and others so that they can be immediately called upon to assist upon discovery of the breach. Also, companies should be prepared for the possibility that the attackers will try to destroy data and interrupt operations, not just steal information. Such attacks are not unheard of, and so health care companies would be wise to check that their continuity of operations plans are up to date.
- **Take Steps to Minimize Legal and Financial Exposures:** The unfortunate reality of an Anthem-like breach is that there will be significant legal and financial exposure. Companies will have to pay regulatory fines, offer credit-monitoring services for persons impacted by the breach, and -- perhaps most costly -- shoulder defense expenses for the inevitable and numerous lawsuits to follow. While it is highly likely that many of the lawsuits will ultimately be dismissed or defeated, the breached company will still face large costs associated with defending themselves in such suits. Companies should thus quickly review their cost-mitigation options to help ensure that when such expenses arise, they have some ability to recoup the associated losses. This would include investigating cyber insurance coverage to help offset any costs incurred as a result of the breach. Companies should also consider applying for liability protections under the SAFETY Act, a federal liability management statute. If nothing else, earning SAFETY Act protections will offer a strong presumption that the company's cyber defenses were "reasonable" and demonstrated diligent efforts to protect its information technology systems.

Data breaches are now a fact of life for companies. Cyber criminals know that their electronic attacks are likely to be both successful and profitable, and therefore no one should expect any drop in the pace or intensity of such attacks. While companies may not be able to stop every data breach, there are steps they can take to minimize the losses associated with such attacks.

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

Pillsbury Winthrop Shaw Pittman LLP