At this point, cyber attacks on politics have transcending the attacks on ordinary industries, like the movies or healthcare companies. But remember, in the days before our concerns about ‘actor states’?

Millions of Anthem Customers Targeted in Cyberattack [2]

Anthem, a major U.S. health insurer, suffers massive hack [3]

And of course, there is this consolation headline

Anthem settles data-breach litigation for record $115 million [4]

But before we go into our happy dance, that a business has been called to account for its lax security reviewing a few facts, dribbled out over time, are in order.

The attorneys general of several states filed a lawsuit over these data breaches. They found that an unnamed nation state was behind the hacks. The why of that is an entirely different topic. [1] But the attorneys general [5] reached a regulatory settlement, no fines, just “make significant investments in security enhancements.” And the report noted other costs by Anthem for the breach, $2.5 million to ‘engage expert consultation,’ and roughly $260 to implement security improvements, notify their customers and public and for credit protection to ‘breach impacted consumers.’

The data-breach litigation heralded above are for a class-action lawsuit addressing the ‘injury’ inflicted on those breach impacted consumers. In the small print, you will find that the $115
number includes some of the costs Anthem agreed to with the attorneys general, but there is an additional $15 million to “pay plaintiffs for out-of-pocket costs due to the breach.”

So, we are looking at about $275 million in spending.

I bring this forward for one reason. Who is paying that bill? Is there a surcharge to each of the company’s stockholders based on the number of shares they own? Doubtful. Are the executives and other members of leadership responsible for the lax security forfeiting their bonus money to pay the fine? Not likely. Is there an insurance fairy who will magically provide the monies? Perhaps, since insurance companies make bets on a broad range of possibilities. But you know the truth, those fines and settlements will come from our pockets, not the perpetrators. The next time you see a big figure settlement with the government, and I am sure this opportunity will come by soon, ask yourself, who is paying this bill? Regulatory fines should punish the actual people behind the transgression otherwise punishment has no meaning. This regulatory fine is a variation on ‘It is easier to apologize than ask permission’ especially when the apology costs you nothing or very little.

[1] It is doubtful that state actors are after your credit card information. Medical records contain sensitive medical information. Information that could be used as leverage to access other accounts that a state actor might more find useful. Or they might run up some great purchases from Amazon.