Cost of a Data Breach for “Company X”

In my example, Company X is a health care provider in the State of Rhode Island. They employ over 15,000 people and run two of the biggest hospitals in the state. Running the biggest hospitals in the state means they hold approximately 300,000 patient records in compliance with HIPAA standards. For this Company X, I will evaluate the total possible costs of a worst-case scenario where all 300,000 patient records were breached, and 15,000 employee records were breached. However, no matter what the size of the breach may be for a particular company, there is still significant consequences, accountability, and damage to reputation to be had.

According to MedPageToday, the average HIPAA violation can cost between $200 and $50,000 per patient record for health care providers who have not put strong security measures in place. For my example, I’ll use the lower end $200 as the multiplier for future fines. Along with the per-patient record fines, in 2013 the Department of Health and Human Services put in place a HIPAA Omnibus rule which says the federal government can an impose a fine of $1.5 million dollars per breach incident. This cost is combined with any that should come with individual patient records being breached. So, for my Company X this means in the worst-case scenario where 300,000 patient records were breached, they could be looking to pay up to $61.5 million dollars in HIPAA violation fines. Unfortunately for Company X the cost doesn’t end there. In the case of a data breach, Company X must also inform every patient, which costs on average $4 per patient. This means an additional cost of around $1.2 million dollars. However, there is still more costs to be accrued. Since medical records are known to contain sensitive personal identifiable information such as social security numbers, this means that the Company X must also provide patients with credit monitoring services. This costs an average of around $10 per patient, so in my worst-case scenario for Company X this adds another $3 million dollars to the total security breach cost. If we add up all the total fines, Company X would be on the hook for around $65 million dollars in total. However, it’s difficult to price out the cost of lost business due to the damaged reputation which is something that can’t be ignored.

Next, we can look at the number of employees on staff and what costs could be incurred if their personal identifiable information where to be breached. According to the text in chapter 3, the Ponemom Institute puts the average cost of a record breach at around $194 dollars. Given that my Company X employs around 15,000 people, it means Company X could look to pay around $3 million in damages. If we include the costs to provide credit monitoring for one year to all employees affected by the breach, Company X is looking at an additional $150,000. This brings the total cost for the employee record breaches to $3.15 million dollars. Therefore, in a worst-case scenario, Company X would have to pay roughly $68.15 million dollars in total to deal with the cost of a data breach. While the number may seem kind of staggering, the average cost for mega breaches (50 – 60 million records) for the health care industry is upwards of $700 million dollars. While I’ve laid out the worst-case scenario here for Company X, as of 2021 the average health care industry data breach costs an average of $9.5 million. Should Company X of had a smaller data breach, we can look to those averages to see what the cost would be.