HealthITSecurity
News and Resources for HealthIT Security Pros

Healthcare Data Breach Costs Still Highest Among Industries

The average healthcare data breach cost is $355 per stolen record, the highest among surveyed industries, according to a recent Ponemon report.

The healthcare industry is no stranger to data breaches, and as technology continues to evolve, covered entities and their business associates need to be especially vigilant when it comes to keeping patient data secure.

A healthcare data breach is also much more likely to cause significant financial damage than security incidents in other sectors, according to a recent study.

The **Ponemon 2016 Cost of Data Breach report**, done in partnership with IBM Security, found that the average cost per stolen record in the healthcare industry was $355—more than twice the average global cost of a stolen record of $158.

"Over the many years studying the data breach experience of more than 2,000 organizations in every industry, we see that data breaches are now a consistent 'cost of doing business' in the cybercrime era," Dr. Larry Ponemon said in a statement. "The evidence shows that this is a permanent cost organizations need to be prepared to deal with and incorporate in their data protection strategies."

Breaches Costlier in Highly Regulated Industries

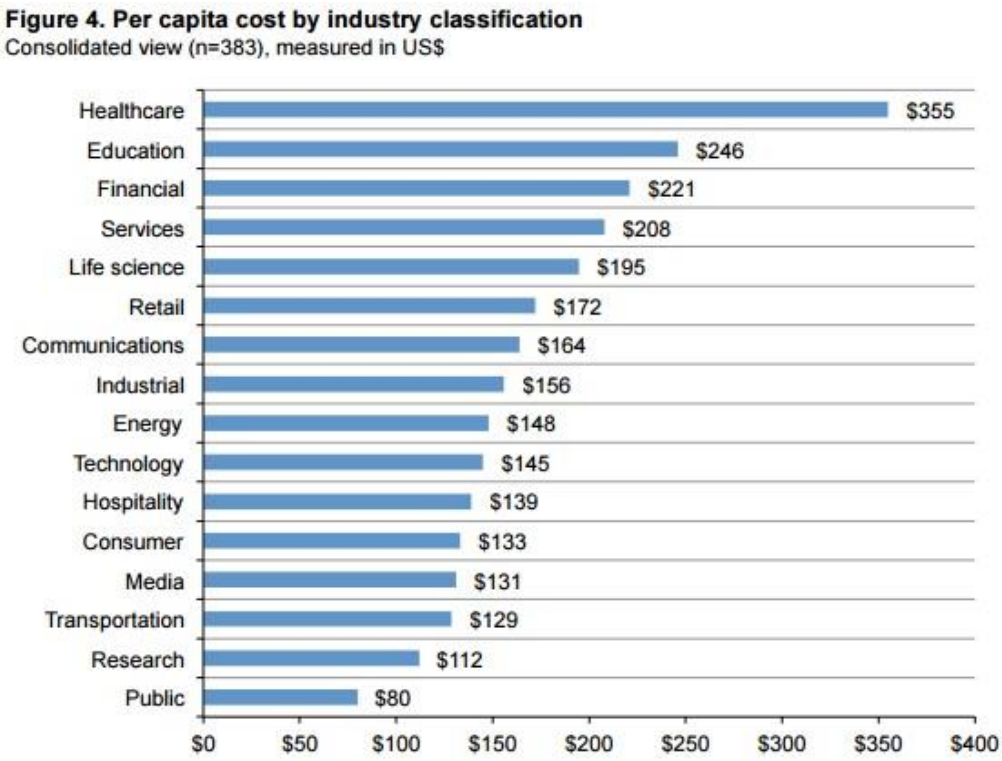
Following healthcare data breaches, the next most expensive cost per stolen record was education at $246, and the financial industry was in third at $221 per stolen record.

"Heavily regulated industries such as healthcare, education and financial organizations had a per capita data breach cost substantially above the overall mean of $158," the report's authors explained.

"Public sector, research and transportation organizations have a per capita cost well below the overall mean value."

Another key takeaway from the report was detection time on data breaches. The longer it takes to detect and then contain a data breach, the more costly it is to resolve the incident. Breaches identified in less than 100 days cost companies an average of $3.23 million, according to Ponemon.

However, breaches that were found after that time cost on average $4.38 million.



Most Breaches Due to Malicious or Criminal Attacks

The majority of data breaches are caused by malicious or criminal attacks, the research shows. This is not only true for incidents in 2016, but has also been a common trend in the 11 years that Ponemon has conducted this research, Dr. Larry Ponemon **explained in a blog post**.

Malicious or criminal attacks also tend to be the more difficult type of breaches to detect, which is why they will also cost more in damages.

For 2016 specifically, 48 percent of all incidents involved a malicious or criminal attack, while 25 percent were caused by negligent employees or contractors (human factor). Finally, 27 percent involved system glitches, including both IT and business process failures.

"In 2016, the cost of data breaches due to malicious or criminal attacks was $170," stated the report's authors. "This is significantly above the per capita cost for breaches caused by system glitch and human factors ($138 and $133, respectively)."

Ponemon also found that certain factors could potentially reduce the cost of a data breach. For example, an incident response team reduced the cost of a data breach by $16, from

$158 to $142. However, third party involvement in the cause of the data breach increased the cost from $158 to $172.

Other types of factors that can potentially reduce the per capita cost include encryption, employee training, participation in threat sharing, or business continuity management.

Extensive cloud migration, a rush to notify, and lost or stolen devices were also top factors that could potentially increase the cost per capita of a data breach.

Breach Stats Similar Between 2015 and 2016

The numbers are similar to the **2015 report**, which showed that healthcare's per capita cost for a data breach was $398, which was still above the overall mean of $217.

Malicious or criminal attacks were also the top cause of data breaches, accounting for 49 percent of reported incidents. System glitches that include IT and business process failures were the root cause of 32 percent of data breaches, and human error accounted for 19 percent.

This article by Elizabeth Snell was published on June 15, 2016 at:
http://healthitsecurity.com/news/healthcare-data-breach-costs-still-highest-among-industries