What Does a Data Breach Really Cost?

Baseline Research Reveals Staggering Direct and Indirect Costs

In 2018, 33 zettabytes of data were generated globally, and this figure has been predicted to reach 175 zettabytes by 2025. The darker side of that is that, according to the Breach Level Index, almost 13.5 billion data records have been lost or stolen in the last six years. The first six months of 2018 alone saw 3.3 billion data records exposed.

To investigate the cost and impact of data breaches, IBM Security and the Ponemon Institute recently published a global overview of their 2018 Cost of a Data Breach Study. In this study, over 2,200 IT, data protection and compliance professionals from 477 companies that had experienced a data breach during 2017 were interviewed. Findings showed that data breaches remain extremely costly and that the impact of such breaches is increasingly painful.

Key Findings of the Poneman Institute Report

Data breaches continue to plague the non-profit sector, private-sector companies and local and national agencies. Although investment in security has increased, the amount of data lost or exposed continues to grow at an even faster rate.

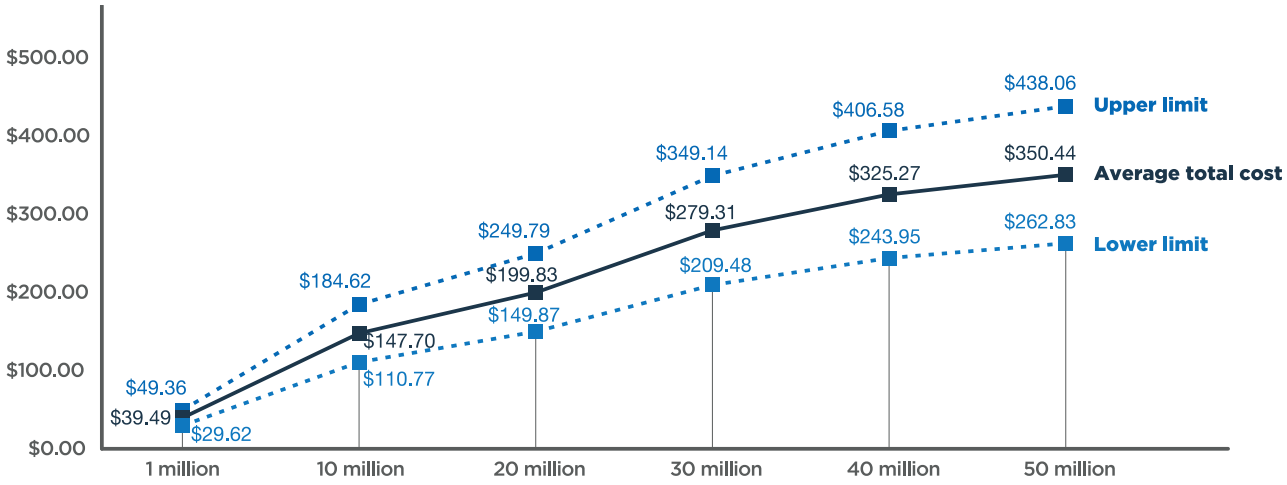
Average total cost of a data breach:	**Average cost per lost or stolen record:**	**Likelihood of a recurring material breach over the next two years:**
$3.86 million	**$148**	**27.9%**
Average total one-year cost increase:	**One-year increase in per capita cost:**	**Average cost savings with an Incident Response team:**
6.4%	**4.8%**	**$14 per record**

The average size of a data breach increased by 2.2% year over year. Unsurprisingly, data breaches were most costly in America ($7.9 million) and the Middle East ($5.3 million), while they cost $3.68 million in the UK, $1.2 million in Brazil and $1.8 million in India. The average cost per record in America was $233, which was the highest of all countries studied. This figure was $202 in Canada and $148 in the UK. America also had the highest notification costs at $740,000; accounting for postal expenditures, email bouncebacks, inbound

communication setups, the engagement of external experts, the creation of contact databases and the determination of regulatory requirements.

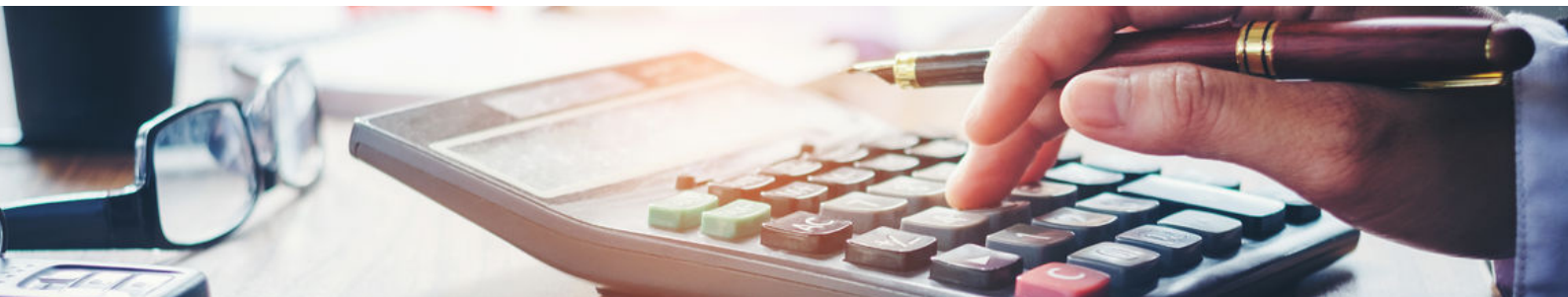
Damage to customer trust in response to data breaches continues to bring the most severe financial consequences. The same Ponemon study found that 65% of consumers lost trust in brands that suffered a data breach. More interestingly, the worst share price performance by publicly listed companies has been seen in companies that had breaches of highly sensitive personal data. The Poneman study supported this, showing that the average share price drop after a breach was 5%.

Costs spiral exponentially when a breach is defined as a "mega breach", which is a data breach that affects over one million records. Mega breaches involving one million records incur an estimated cost of $39.49 million, with a range from $29.62 to $49.36 million. At 50 million records, the cost is estimated to be $350.44 million, with a range from $262.83 to $438.06 million..



As shown in the table below, many costs are involved in addressing and recovering from a mega breach.

Number of breached records	Detection & escalation	Notification	Post data breach response	Lost business cost	Total cost
1,000,000	$ 11,682,870	$ 567,130	$ 12,225,694	$ 15,012,731	$ 39,488,426
10,000,000	$ 44,851,852	$ 1,878,009	$ 48,039,120	$ 52,926,157	$ 147,695,139
20,000,000	$ 62,481,481	$ 3,174,306	$ 67,170,833	$ 67,005,556	$ 199,832,176
30,000,000	$ 88,407,407	$ 4,151,389	$ 91,763,194	$ 94,989,352	$ 279,311,343
40,000,000	$ 102,537,037	$ 5,903,009	$ 106,411,343	$ 110,413,657	$ 325,265,046
50,000,000	$ 110,998,725	$ 6,498,576	$ 115,028,472	$ 117,919,213	$ 350,444,986



Let TES Be Your Guide

Data breaches are expensive and only getting more so. The General Data Protection Regulation (GDPR) in the European Union and data protection regulations in the United States and other countries mean that organisations are legally mandated to have a regimented plan in place to ensure the security of private citizens' data. In that context it is important to note that while front-end cyber security lapses are at the forefront of data breaches in the news, there are many examples of breaches caused by the improper retirement of IT assets that contain data.

The vast majority of breaches involve a failure to apply technology properly or a failure to follow documented processes. The embedded risks around these breaches must be managed and only providers with true scale have the resources and expertise to meet this challenge; a challenge that becomes infinitely more complex with the addition of national, regional and local regulations across the global landscape. TES is one of the few providers that owns / operates its own worldwide processing network (30+ locations across 20 countries) and our knowledge of the global regulatory environment means that we can guide organisations through the minefields that surround their technology asset disposition procedures.

It's a big world out there, but it doesn't have to feel that way.

Let TES be your guide—contact us to discuss your IT lifecycle needs in more detail.

info@tes-amm.com
www.tes-amm.com