WERKSMANS
ATTORNEYS

REGULATORY

# Average data breach costs SA companies R50m

20 September 2019 *3 min read*

With data breaches becoming commonplace it seems as if businesses need to now consider not whether they will be victims of a data breach but rather when.

People doing business with any company expect them to keep their data safe. So when there is a data breach it results in not only a large cost to the company but also a massive loss of trust by clients, many of whom will never deal with the company again.

Recent research by the US's Ponemon Institute, which conducts independent research on data protection, showed that a data breach costs South African companies on average $3.06m or nearly R50m. By comparison, the average data breach in the UK costs $3.88m (R60m), Germany $4.78m (R73m) and in the United States, $8.19m (R130m), the most of all countries.

The costs of data breaches are so high because there are four cost components to any data breach:

1. Detection and escalation; which are activities that enable companies to detect and report the breach.
2. Notification; the activities the company must undertake to notify people whose data has been compromised, as well as informing regulators.
3. Post data breach response; processes to help customers communicate with the company and also the related costs of redress
4. Lost business; the largest single cost of a date breach at 36% of total cost. This includes lost business such as revenue loss, business disruption, system downtime and customer acquisition.

The research also showed that globally, the average cost of lost business after a data breach was $1.42m (R22m.)

When surveyed by Gemalto, a Dutch digital security company, nearly two-thirds of people indicated that they would likely end their relationship with a business after their personal information had been exposed. Such is the strong negative correlation between data breaches and customer loyalty.

But it's not just a once off event and then it's business as usual. There is an insidious long tail impact too that most organisations are not prepared for. Not only will a business likely continue to bleed customers for years after a breach, but it also deters customers who were considering using the company such is the damage to brand and reputation.

Can new customers be acquired?

Yes, but at a much higher cost than before the breach. This higher cost of acquisition is a long term phenomenon and an ongoing cost for companies which reduces profits. When businesses consider the full impact of a breach, they are likely to take much greater care to prevent it happening.

**Ahmore Burger-Smidt**

Head of Regulatory

View Profile