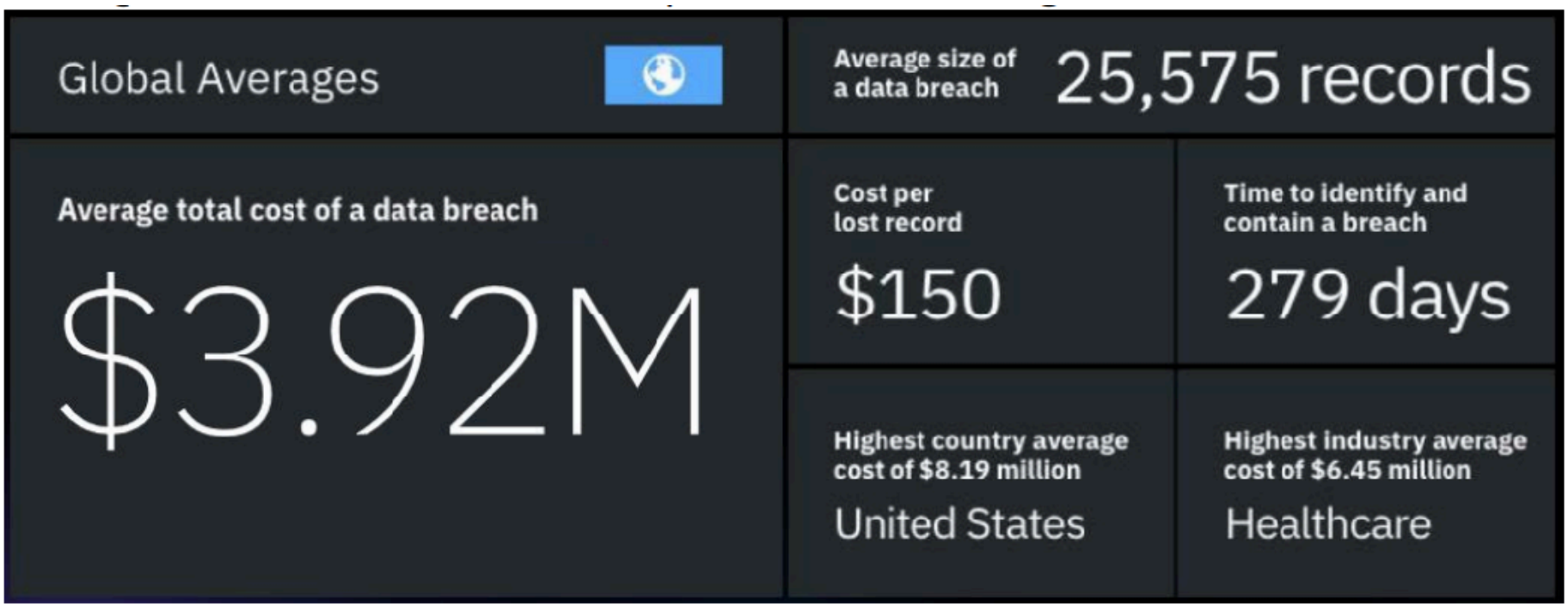
Enterprise Level Damage Due to any Data Breach

Bookmark this page

A data breach is defined as an event in which an individual's name and a medical record and/or a financial record or debit card is potentially put at risk, either in electronic or paper format. In our study, we identified three main causes of a data breach: malicious or criminal attack, system glitch or human error. The costs of a data breach vary according to the cause and the safeguards in place at the time of the data breach.

A data breach can have far-reaching consequences, causing financial losses and affecting an organization's operations and compliance in the short term. And a major breach in the headlines can potentially damage reputation for years to come, leading to lost business and a competitive disadvantage.



How the cost of a data breach is calculated To calculate the cost of a data breach, we use an accounting method called activitybased costing (ABC). This method identifies activities and assigns a cost according to actual use. The ABC methodology is fully explained in the How We Calculate the Cost of a Data Breach section of this report. Four process-related activities drive a range of expenditures associated with an organization's data breach detection, escalation, notification and post data breach response. The four cost centers are described below.