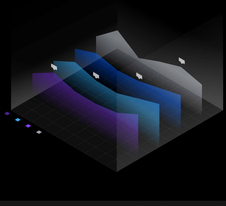
Cost of a Data Breach Report 2020



Highlights from the report based on a study of 500+ data breaches. Conducted by Ponemon Institute, analyzed and published by IBM Security.

Data breach costs diverged

The global average cost of a data breach declined slightly in 2020, but costs were much higher than average in some organizations based on factors such as geography, industry and level of security maturity.

$3.86M

Global average total cost of a data breach

↓1.5%

Change in average total cost, 2019-2020

Security automation saved millions

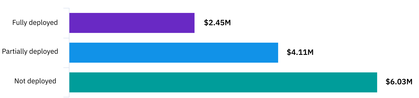
Security automation – using technologies such as AI, analytics and automated orchestration – was most effective at mitigating data breach costs.

$3.58M

Reduction in average total cost for fully deployed vs. no security automation

Average total cost by security automation level

Measured in US$



Customer PII drove costs higher

Customer personally identifiable information (PII) was the most commonly exposed type of data with the most expensive cost per record (vs. intellectual property, employee data or anonymized customer data).

80%

Share of breaches with customer PII

$175

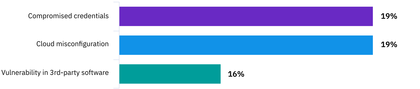
Average cost per record of customer PII (in malicious attacks)

Compromised credentials and cloud misconfiguration led the way

Compromised credentials (19%) and cloud misconfiguration (19%) were the most common causes of malicious breaches and among the top three costliest along with vulnerabilities in third-party software. These were also the most expensive initial attack vectors by average total cost.

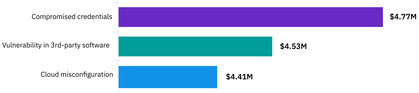
Top initial attack vectors

As a percentage of all malicious breaches



Costliest initial attack vectors

Average total cost in US$



Nation state attacks: Less common, but costliest

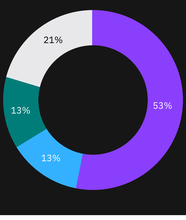
Nation state actors caused 13% of malicious breaches, while 53% were caused by financially motivated attackers. However, nation state attacks were costliest.

Which threat actors were costliest?

Average total cost in US$

- Nation state $4.43 million
- Unknown $4.29 million
- Hacktivist $4.28 million
- Financially motivated $4.23 million

Share of malicious breaches per threat actor type

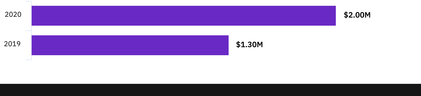


Effectiveness of incident response grew

Organizations that had an incident response (IR) team and tested their IR plans averaged breach costs of $3.29 million, compared to $5.29 million for organizations with neither IR teams or IR testing.

Cost saving for organizations with IR team and IR testing

Measured in US$



Mega breaches, mega costs

Data breaches of more than 1 million records, or "mega breaches," are not experienced by most organizations, but they have an outsized impact on customers and industries.

12x-100x

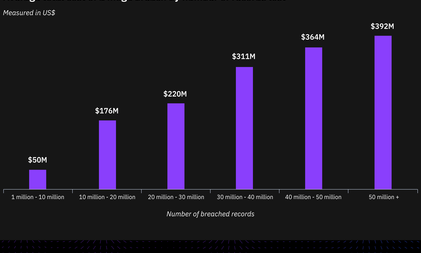
Multiplier of mega breach costs vs. the average data breach

$392M

Average cost of a mega breach of 50 million+ records

Average total cost of a mega breach by number of records lost

Measured in US$



Explore the report and calculator

ibm.com/databreach →