Cost of a Data Breach Report 2020

See the report and calculator

Scroll for highlights

$3.86M

Global average total cost of a data breach in 2020

$7.13M

Healthcare has the highest industry average cost.

$150

Customer PII data has the highest cost per record.

$8.64M

United States has the highest country average cost.

IBM

Ponemon INSTITUTE

Security >

How much would a data breach cost your business?

The 2020 Cost of a Data Breach Report explores financial impacts and security measures that can help your organization mitigate costs

→ Register for report and calculator

Cost of a Data Breach Report 2020

Review key findings and best practices. See how much a data breach might cost your business and how to mitigate potential damages.

Register for webinar

If you are experiencing a cybersecurity incident, contact the X-Force team to help

US hotline 1-888-241-9812

Global hotline (+001) 312-212-8034

→ Learn more about incident response services

Cost of a Data Breach Report highlights

USD 3.86 million

Average total cost of a data breach

United States

Most expensive country: USD 8.64 million

Healthcare

Most expensive industry: USD 7.13 million

280 days

Average time to identify and contain a breach

Calculate breach costs by industry and geography

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.

Independently conducted by the Ponemon Institute, and based on quantitative analysis of 524 recent breaches across 17 geographies and 17 industries, the annual Cost of a Data Breach Report offers exceptional insights and benchmarks to help organizations improve security posture and mitigate financial and brand damages.

→ Register for the report and cost calculator

Align your security strategy with your business

→ IBM Security Services

Protect your digital assets, users and data

→ Identity and access management

→ Data security

Manage your defenses against growing threats

→ Security information and event management (SIEM)

→ Security orchestration, automation and orchestration (SOAR)

Modernize your security with an open, multicloud strategy

→ Cloud security

Looking for past reports? Find them here.

2019 Cost of a Data Breach Report

→ Register for the report

2018 Cost of a Data Breach Report

→ Register for the report

2017 Cost of a Data Breach Report

→ Register for the report

Discover more research reports

X-Force Threat Intelligence Research Hub

Threat intelligence, research and reports for a preemptive approach to cyber security.

→ Explore research

Cloud Security Landscape Report

The latest cloud threats and best practices to defend against those threats.

→ Register for report

2020 Cost of Insider Threats report

An independent study on how security leaders can mitigate insider breaches.

→ Learn about insider threat costs

DATA INSIDER BLOG

What's the Cost of a Data Breach in 2019?

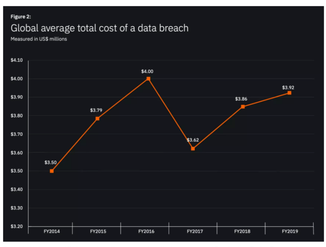
by Chris Brook on Tuesday July 30, 2019

The answer ultimately depends on the country and industry but in general, can span anywhere from $1.25 million to $8.19 million.

It's difficult to get a proper grip on cybersecurity by the numbers, especially when every other day brings news of a new breach, many which see millions upon millions of records exposed.

The latest number - one that's a safe bet to change in a few months from now, if not sooner - is $3.9 million.

That's the average cost of a data breach currently, a figure that's up 1.5 percent from the year prior and factors into a 12 percent increase over the past five years.



The statistic, per IBM and the Ponemon institute's annual "**Cost of a Data Breach**" report, will likely be one of the most cited, the rest of the year, across the cybersecurity landscape, when it comes to putting a price tag on the costs associated with a breach.

The report, which clocks in at 77 pages this year, aggregates costs reported by 507 organizations, from 17 industries, from 16 regions: United States, India, the United Kingdom, Germany, Brazil, Japan, France, the Middle East, Canada, Italy, South Korea, Australia, Turkey, ASEAN, South Africa, and, Scandinavia. Through interviews with 3,211 individuals, IBM and Ponemon collected data points regarding the number of customer records lost or stolen in breaches, how the company responded to the breach, and how their business fared after the breach. The report, released last week, is in its 14th year.

According to the report, data breaches cost companies surveyed in the report $150 per record. Perhaps unsurprisingly, that number is up over last year's figures, which put the average cost of each record at $148, up from $141 in 2017.

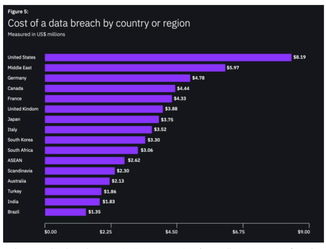
Can Factors Detract From the Cost of a Data Breach?

The report thoroughly breaks down every angle of a data breach and at one point, digs into how having mitigations in place, like an incident response team or encryption, can reduce the cost of a breach. According to IBM/Ponemon, by having both in place a company could potentially reduce the cost of a breach by $720,000.

According to the report, companies that had security automation technologies deployed experienced around half the cost of a breach ($2.65 million on average) compared to those that did not have these technologies deployed ($5.16 million average). Specifically, companies that have an incident response team and build on that team by performing periodic incident response plan testing proved beneficial too; companies that do both could save $1.23 million per data breach on average, according to the report.

The U.S. Is #1

It's important to note that these numbers are an average and not the norm in the United States, the most expensive country in which to experience a data breach.

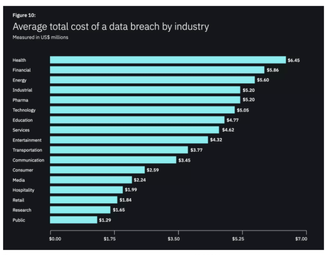


In the U.S. a data breach costs a company on average $8.19 million, an increase from $7.91 million in 2018, and more than twice the global average. The cost per breached record, $242, is steeper too.

Where the U.S. wasn't tops, was the average number of records per breach. According to the report, orgs in both the Middle East and India (38,800 and 35,636) had more records exposed per breach than the U.S.

Healthcare Breach Woes

The **healthcare industry** has proven time and time again to be a susceptible target for attackers when it comes to cyberattacks and this report's numbers surely complement that concept. According to the report, healthcare breaches cost organizations $6.45 million per breach, a number that eclipses all other sectors and makes it the ninth year in a row that healthcare orgs have had the highest costs associated with a data breach.



The average cost for per breached healthcare record ($429) is more than double any other industry too and substantially higher than the average, $150, according to the report.

Unfortunately, according to IBM and Ponemon's statistics, healthcare breaches can often take the longest to identify, up to 236 days; they take the longest, tied with attacks on the public infrastructure, to remedy as well.

The healthcare industry (followed by the financial and pharmaceuticals industries) had the biggest difficulty retaining customers following a breach. On average, the abormal customer turnover is 3.9 percent; for health companies, it was 7.0 percent.

Tags: **Data Breaches**

CHRIS BROOK

Chris Brook is the editor of Data Insider. He is a technology journalist with a decade of experience writing about information security, hackers, and privacy. Chris has attended many infosec conferences and has interviewed hackers and security researchers. Prior to joining Digital Guardian he helped launch Threatpost, an independent news site which is a leading source of information about IT and business security for hundreds of thousands of professionals worldwide.

Related Blog Posts

For Data Thieves, the Internet of Easy Pickings
Paul Roberts

Data Theft and DDT: Courts Increasingly Back 'Future Risk' from Data Breaches
Paul Roberts

Friday Five: 9/20 Edition
Chris Brook