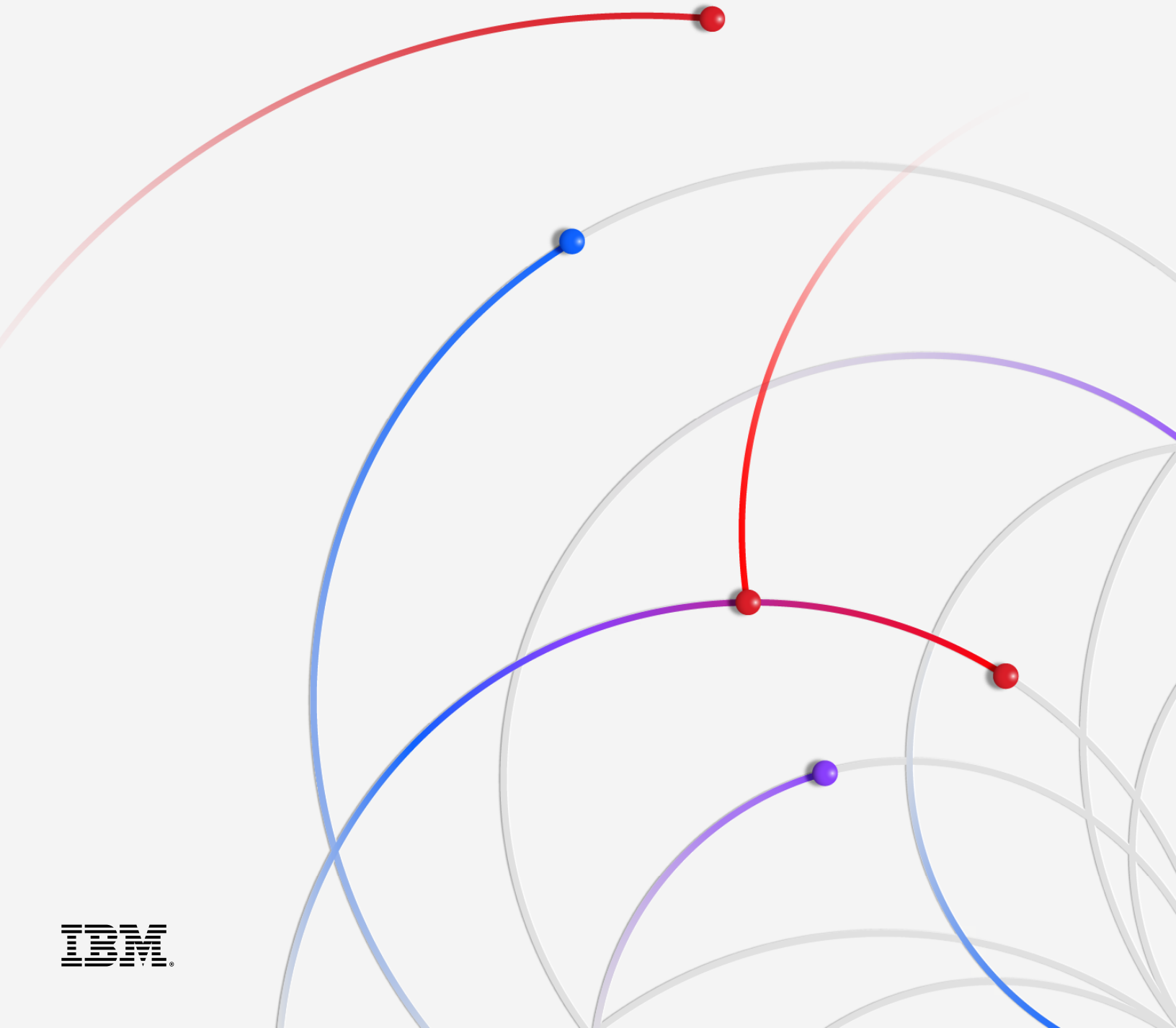
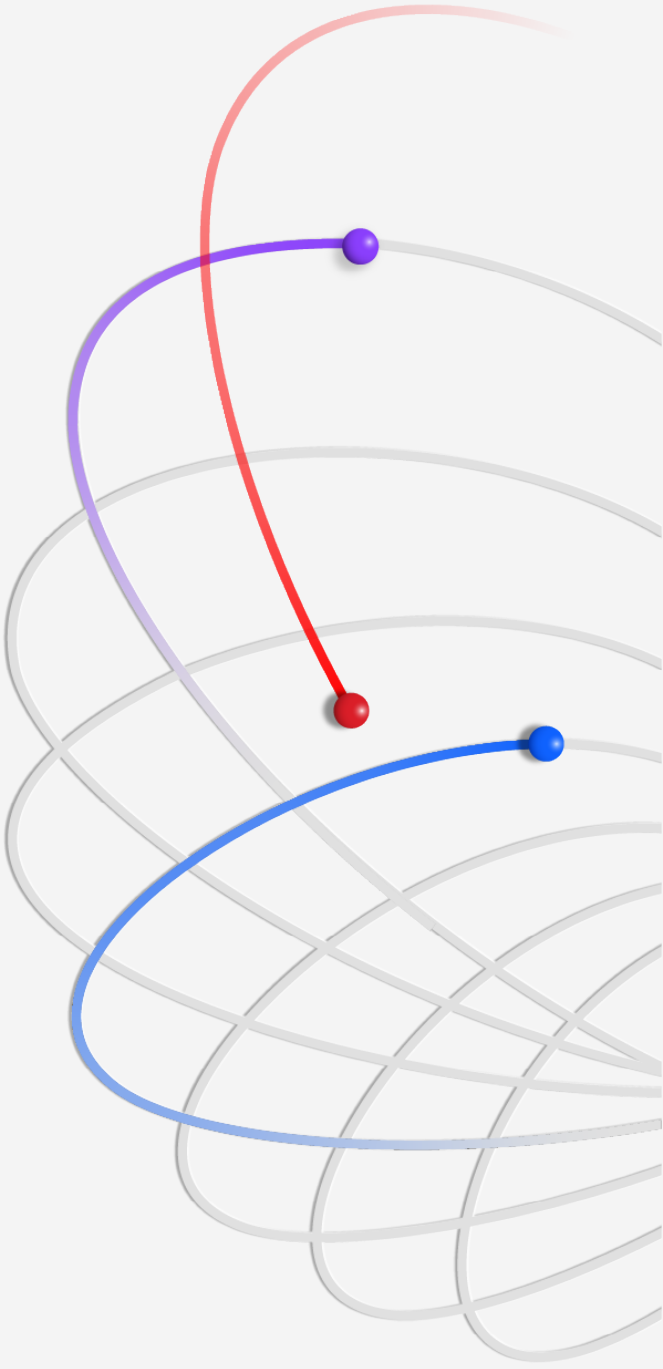
Cost of a Data Breach Report 2024



IBM

Table of contents

Executive summary



IBM's annual Cost of a Data Breach Report provides IT, risk management and security leaders with timely, quantifiable evidence to guide them in their strategic decision-making. It also helps them better manage their risk profiles and security investments. This year's report—the 19th of the series—reflects changes caused by technological shifts, such as the rise of shadow data, which is data residing in unmanaged data sources, and the extent and costs of business disruption brought about by data breaches.

The report's research—conducted independently by Ponemon Institute and sponsored, analyzed and published by IBM—studied 604 organizations impacted by data breaches between March 2023 and February 2024. Researchers looked at organizations across 17 industries, in 16 countries and regions, and breaches that ranged from 2,100 to 113,000 compromised records. To gain on-the-ground insights, Ponemon Institute researchers interviewed 3,556 security and C-suite business leaders with firsthand knowledge of the data breach incidents at their organizations.

The result is a benchmark report that business and security leaders can use to strengthen their security defenses and drive innovation, particularly around the adoption of AI in security and security for their generative AI (gen AI) initiatives.

We lead this year's report with 2 major developments. First, the global average cost of a data breach increased 10% over the previous year, reaching USD 4.88 million, the biggest jump since the pandemic. Business disruption and post-breach customer support and remediation drove this cost spike. When asked how they're dealing with these costs, more than half of organizations said they are passing them on to customers. Having customers absorb these costs can be problematic in a competitive market already facing pricing pressures from inflation.

Second, on the defender side of the equation, researchers also found applying security AI and automation is paying off, lowering breach costs in some instances by an average of USD 2.2 million. AI and automation solutions are reducing the lifespan needed to identify and contain a breach and its resulting damage. Put another way, defenders without AI and automation to assist them can expect to take longer to detect and contain a breach, and see costs rise compared to those who use these solutions.

As we've seen across the industry, cybersecurity teams are consistently understaffed. This year's study found more than half of breached organizations faced severe security staffing shortages, a skills gap that increased by double digits from the previous year. This lack of trained security staff is growing as the threat landscape widens. The continuing race to adopt gen AI across nearly every function in the organization is expected to bring with it unprecedented risks and put even more pressure on these cybersecurity teams.

This report provides insights and recommendations from the research to help reduce the potential financial and reputational damages from a data breach.

What's new in the 2024 report

Each year, we continue to evolve the Cost of a Data Breach Report to reflect new technologies, emerging tactics and recent events. For the first time, this year's research explores:

- Whether organizations experienced long-term operational disruption, for example, the inability to process sales orders, a complete shutdown of production facilities, ineffective customer services
- Whether the breach included data stored in unmanaged data sources, otherwise known as shadow data
- To what extent organizations are using AI and automation in each of 4 areas of security operations: prevention, detection, investigation and response
- The nature of extortion attacks, for example, extortion and ransomware attacks or extortion and data exfiltration only
- The time it takes to restore data, systems or services to their pre-breach state
- How long it took organizations to report the breach if they were mandated to do so
- Whether organizations that involved law enforcement following a ransomware attack paid the ransom

Key findings

The key findings described here are based on IBM analysis of research data compiled by Ponemon Institute.

USD 4.88M

Average total cost of a breach
The average cost of a data breach jumped to USD 4.88 million from USD 4.45 million in 2023, a 10% spike and the highest increase since the pandemic. A rise in the cost of lost business, including operational downtime and lost customers, and the cost of post-breach responses, such as staffing customer service help desks and paying higher regulatory fines, drove this increase. Taken together, these costs totaled USD 2.8 million, the highest combined amount for lost business and post-breach activities over the past 6 years.

USD 2.2M

Cost savings from extensive use of AI in prevention
2 out of 3 organizations studied stated they're deploying security AI and automation across their security operations center, a 10% jump from the prior year. When deployed extensively across prevention workflows—attack surface management (ASM), red-teaming and posture management—organizations averaged USD 2.2 million less in breach costs compared to those with no AI use in prevention workflows. This finding was the largest cost savings revealed in the 2024 report.

26.2%

Growth of the cyber skills shortage
More than half of breached organizations are facing high levels of security staffing shortages. This issue represents a 26.2% increase from the prior year, a situation that corresponded to an average USD 1.76 million more in breach costs. Even as 1 in 5 organizations say they used some form of gen AI security tools—which are expected to help close the gap by boosting productivity and efficiency—this skills gap remains a challenge.

1 in 3

Share of breaches involving shadow data
35% of breaches involved shadow data, showing the proliferation of data is making it harder to track and safeguard. Shadow data theft correlated to a 16% greater cost of a breach. Researchers found storing data across environments proved to be a common storage strategy, accounting for 40% of breaches. These breaches also took longer to identify and contain. In contrast, data stored in just 1 type of environment was breached less often, whether that environment was public cloud (25%), on premises (20%) or private cloud (15%).

USD 4.99M

Average cost of a malicious insider attack
Compared to other vectors, malicious insider attacks resulted in the highest costs, averaging USD 4.99 million. Among other expensive attack vectors were business email compromise, phishing, social engineering and stolen or compromised credentials. Gen AI may be playing a role in creating some of these phishing attacks. For example, gen AI makes it easier than ever for even non-English speakers to produce grammatically correct and plausible phishing messages.

46%

Share of breaches involving customer personal data
Nearly half of all breaches involved customer personal identifiable information (PII), which can include tax identification (ID) numbers, emails, phone numbers and home addresses. Intellectual property (IP) records came in a close second (43% of breaches). The cost of IP records jumped considerably from last year, to USD 173 per record in this year's study from USD 156 per record in last year's report.

USD 1M

Cost savings when law enforcement is involved in ransomware attacks
Ransomware victims that involved law enforcement ended up lowering the cost of the breach by an average of nearly USD 1 million, and that excludes the cost of any ransom paid. Involving law enforcement also helped shorten the time required to identify and contain breaches from 297 days to 281 days.

292

Days to identify and contain breaches involving stolen credentials
Breaches involving stolen or compromised credentials took the longest to identify and contain (292 days) of any attack vector. Similar attacks that involved taking advantage of employees and employee access also took a long time to resolve. For example, phishing attacks lasted an average of 261 days, while social engineering attacks took an average of 257 days.

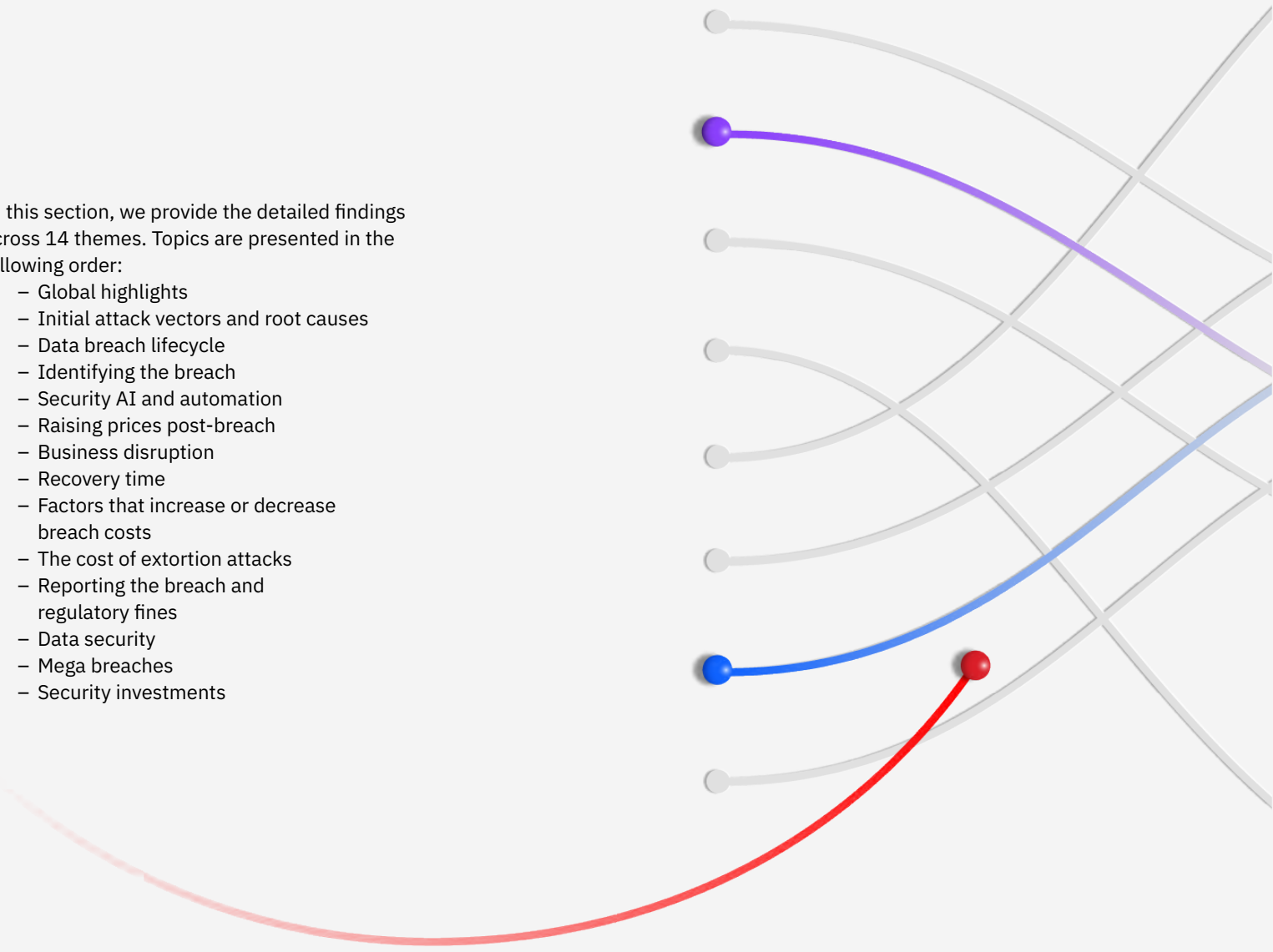
USD 830,000

Largest average cost increase among all industries
The industrial sector experienced the costliest increase of any industry, rising by an average USD 830,000 per breach over last year. This cost spike could reflect the need for industrial organizations to prepare for a more rapid response, as organizations in this sector are highly sensitive to operational downtime. Still, the time to identify and contain a data breach at industrial organizations was above the median industry, at 199 days to identify and 73 days to contain.

Complete findings

In this section, we provide the detailed findings across 14 themes. Topics are presented in the following order:

- Global highlights
- Initial attack vectors and root causes
- Data breach lifecycle
- Identifying the breach
- Security AI and automation
- Raising prices post-breach
- Business disruption
- Recovery time
- Factors that increase or decrease breach costs
- The cost of extortion attacks
- Reporting the breach and regulatory fines
- Data security
- Mega breaches
- Security investments



USD 4.88M

The global average cost of a data breach spikes

Global highlights

Globally, security teams are doing a much better job of detecting and containing breaches, despite a stubborn skills shortage. More than half of breached organizations are facing security staffing shortages, and security leaders are, in turn, marshalling AI and automation solutions to close the skills gap. Despite their efforts, breach costs are rising, mostly from expenses related to business disruption and post-breach responses. In the following section, we look at these issues and others, across industries, countries and regions, to provide security leaders with a view of the risks out there so you can learn from them.

The global average cost of a data breach spiked

The global average cost of a data breach increased 10% in one year, reaching USD 4.88 million, the biggest jump since the pandemic. Business disruption and post-breach response activities drove most of this yearly cost increase. See Figure 1.

Global average total cost of a data breach

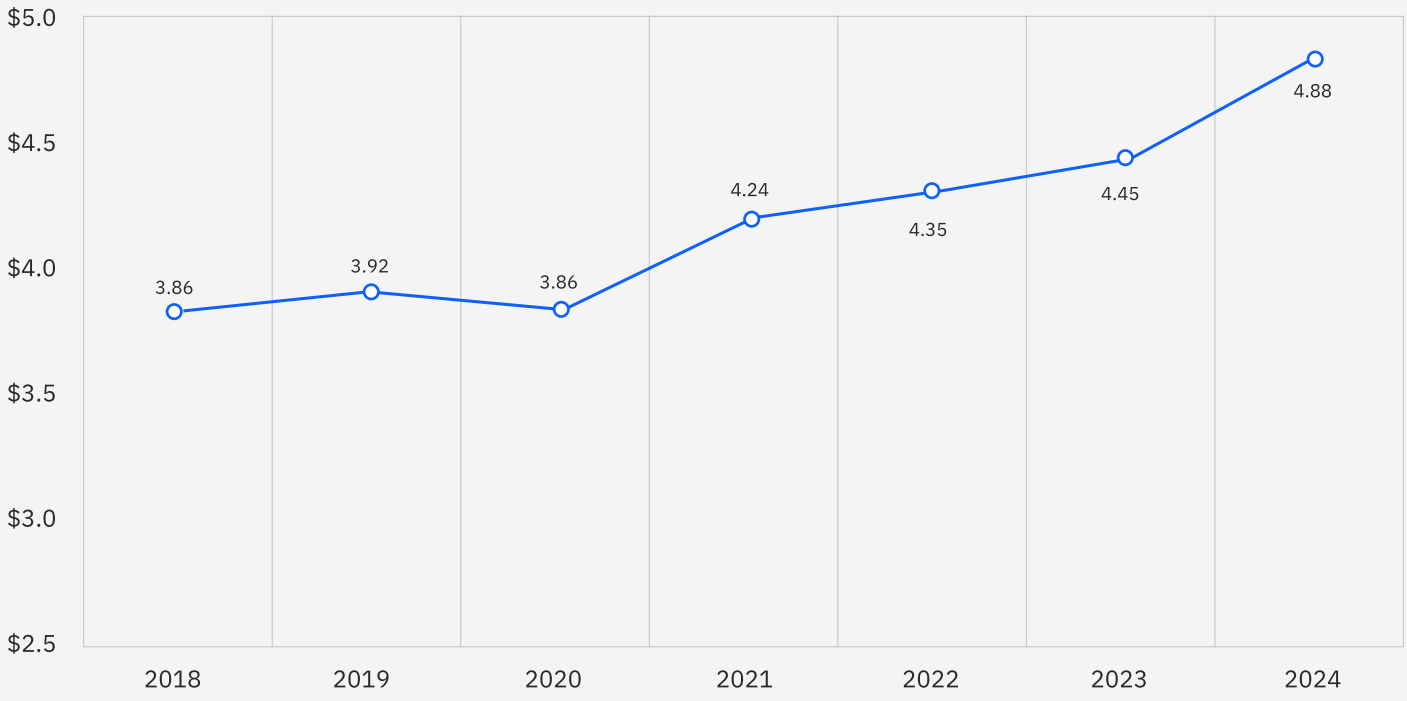


Figure 1. Measured in USD millions

The United States led the world in average breach cost
For the 14th year, the United States had the highest average data breach cost—USD 9.36 million—among the 16 countries and regions studied. Rounding out the top 5 were the Middle East, Germany, Italy and Benelux. Benelux is the economic union of Belgium, the Netherlands and Luxembourg, and it's a new addition this year. Notably, Canada and Japan saw average costs drop, while Italy and the Middle East saw significant increases. See Figures 2A and 2B.

Cost of a data breach by country or region

#	Country	2024	2023
1	United States	$9.36	$9.48
2	Middle East	$8.75	$8.07
3	Benelux	$5.90	—
4	Germany	$5.31	$4.67
5	Italy	$4.73	$3.86
6	Canada	$4.66	$5.13
7	United Kingdom	$4.53	$4.21
8	Japan	$4.19	$4.52
9	France	$4.17	$4.08
10	Latin America	$4.16	$3.69
11	South Korea	$3.62	$3.48
12	ASEAN	$3.23	$3.05
13	Australia	$2.78	$2.70
14	South Africa	$2.78	$2.79
15	India	$2.35	$2.18
16	Brazil	$1.36	$1.22

Figure 2A. Measured in USD millions

Top 5 countries and regions 2024 vs 2023

#	Cost change	2024	2023
1	↓	**United States** $9.36	**United States** $9.48
2	↑	**Middle East** $8.75	**Middle East** $8.07
3	↑	**Benelux** $5.90	**Canada** $5.13
4	↑	**Germany** $5.31	**Germany** $4.67
5	↑	**Italy** $4.73	**Japan** $4.52

Figure 2B. Measured in USD millions

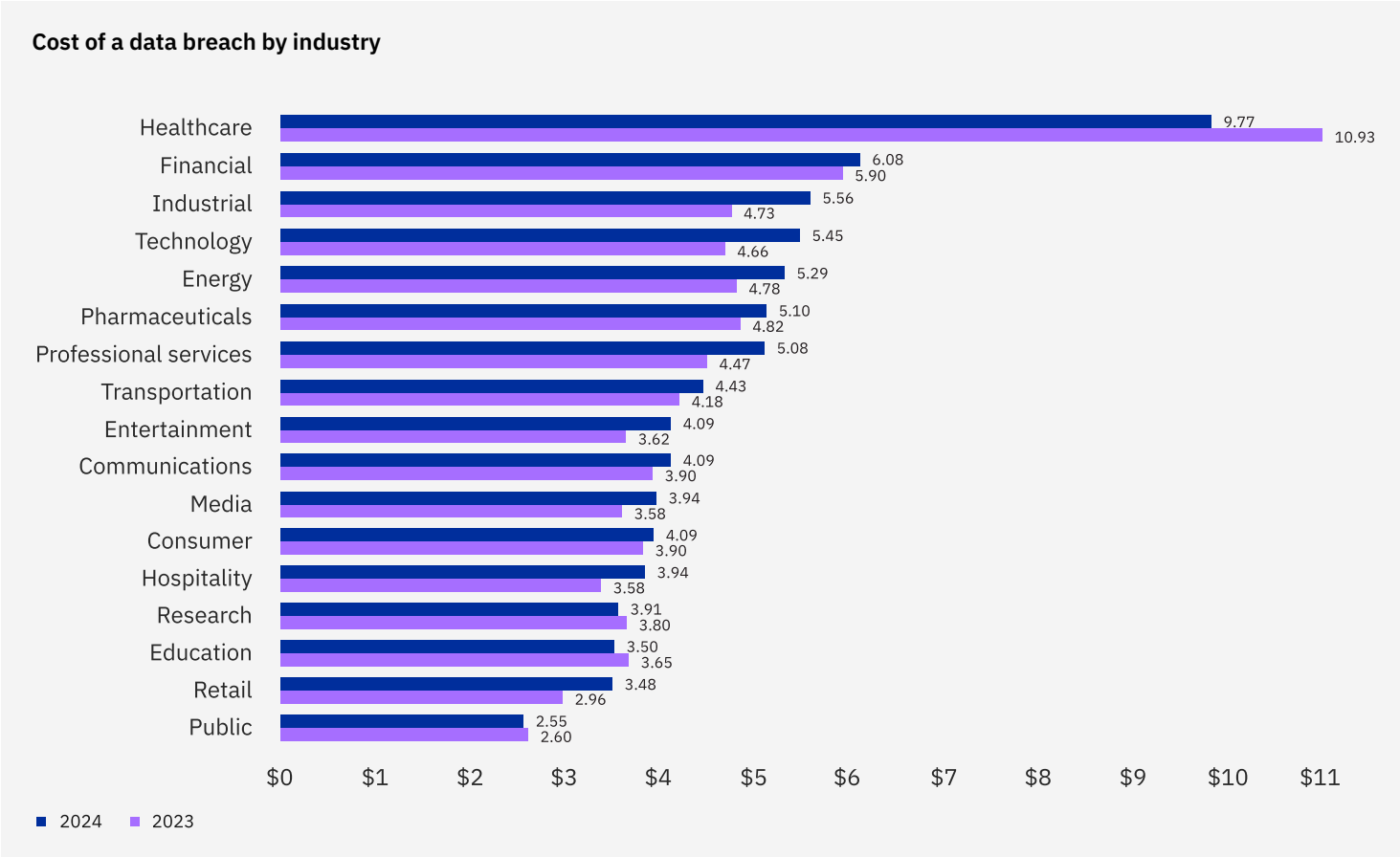


Figure 3. Measured in USD millions

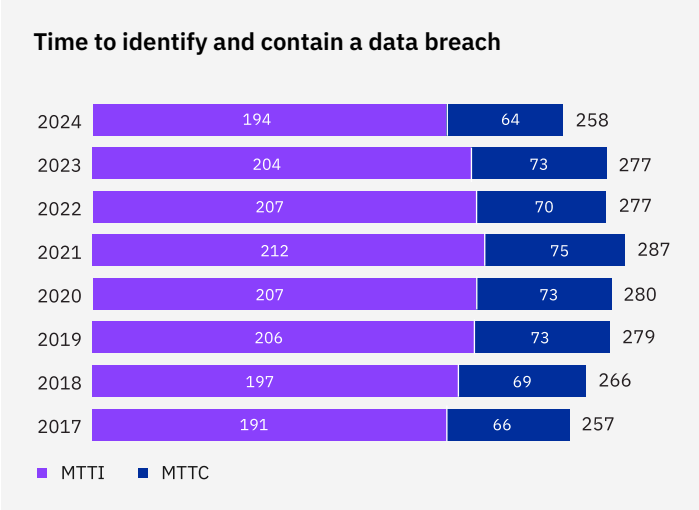


Figure 4. Measured in days

Healthcare topped industry costs, again

The average breach cost for healthcare fell 10.6%, to USD 9.77 million. But that factor wasn't enough to remove it from the top costliest industry for breaches—a spot it's held since 2011. Healthcare remains a target for attackers since the industry often suffers from existing technologies and is highly vulnerable to disruption, which can put patient safety at stake. See Figure 3.

Average time to identify and contain a breach fell

The mean time it took defenders to identity and contain a breach dropped to 258 days, reaching a 7-year low, compared to 277 days the previous year. Note: this global average of mean time to identify (MTTI) and mean time to contain (MTTC) excludes Benelux because, as a new region in the study, it was having outsized influence and skewed results much more than the average. See Figure 4.