ELEVATE
SOLUTIONS

REPORT · BUSINESS & INDUSTRY

The True Cost of a Data Breach

By industry, by controls

What a breach actually costs — IBM's latest figures broken down for smaller firms, and the controls that measurably reduce the number.

01 — COST BY INDUSTRY

What a breach costs, by the numbers that exist

IBM's Cost of a Data Breach Report is the benchmark most boards, carriers, and counsel reach for. Every figure in this report comes from that study or from the other named sources cited inline. Where no published figure exists, this report says so instead of inventing one.

$4.44M
Global average breach cost
IBM 2025

$10.22M
US average — a record high
IBM 2025

$7.42M
Healthcare average
IBM 2025

The global average breach cost is $4.44M, down 9% from $4.88M the year before. IBM Cost of a Data Breach Report 2025 The decline tracks faster response: the mean time to identify and contain a breach fell to 241 days, a 9-year low. IBM Cost of a Data Breach Report 2025

The United States moved the other way. The US average is $10.22M — a record high. IBM Cost of a Data Breach Report 2025 US breaches are expensive for structural reasons: state-by-state notification statutes, active regulators, a plaintiffs' bar that files quickly, and clients who are themselves regulated and must report their vendors' incidents.

Healthcare remains the costliest industry at $7.42M on average — the costliest 14 years running. IBM Cost of a Data Breach Report 2025 Healthcare breaches also run longer: a 279-day average lifecycle against the 241-day all-industry mean. IBM Cost of a Data Breach Report 2025 Records that cannot be reissued, systems that cannot be taken offline, and a federal regulator with its own breach portal all extend the clock.

Why regulated industries pay more

The premium that legal, healthcare, and financial firms pay over the average is structural, not bad luck. Five drivers do most of the work:

COST DRIVER	WHY IT SCALES IN A REGULATED FIRM
Notification	Statutes — HIPAA, state breach laws, professional-conduct rules — decide who must be told and how fast. Mailings, call centers, and translation are billed per affected person, and regulated data tends to cover everyone in the file.
Regulator response	Investigations, document production, interviews, and corrective-action plans consume partner and executive hours for months after the technical incident is closed. Penalties, where they come, arrive on top.
Credit monitoring	Offering monitoring to affected individuals is standard practice and often a regulator expectation. The cost multiplies by headcount of records, not by company size.
Litigation	Breaches of regulated data attract class actions and individual client claims. Defense costs accrue regardless of outcome, and privilege fights over the forensic report add their own track.

Client attrition	Clients with their own compliance duties must reassess any vendor that loses their data. Referral sources pause. In professional services, the lost lifetime value of departed clients can outlast every other line item.

WHAT THE AVERAGE HIDES

An average mixes mega-breaches with contained incidents. Your number depends on how many records you hold, how long you can operate without your systems, and which notification and regulatory duties attach to your data — not on your revenue. The sections that follow deal with each of those levers.

02 — COST BY COMPANY SIZE

What is actually known about smaller firms

Most breach statistics describe large enterprises. Here is what is published about smaller organizations — and, just as important, what is not.

IBM's current report does not break out cost by company size. The last edition to publish a by-size breakdown was the 2023 report. In it, organizations under 500 employees averaged $3.31M per breach. IBM Cost of a Data Breach Report 2023 Treat that as the most recent published figure, not a current one. There is no newer by-size number from IBM, and this report will not manufacture one.

$3.31M

Average breach cost, organizations under 500 employees

IBM 2023 — last published by-size breakdown

Why the per-employee impact is worse when you are small

A smaller firm does not get a smaller breach. Most of the cost is fixed, and the fixed parts hit hardest where there is least slack:

COST COMPONENT	HOW IT LANDS ON A SMALLER FIRM
Forensics	Incident-response firms staff and bill the same specialists whether the victim has fifty employees or five thousand. The retainer, the imaging, and the report do not scale down with headcount.
Breach counsel	Notification analysis is jurisdiction-by-jurisdiction legal work. A small client list spread across several states generates the same statutory matrix as a large one.
Notification vendors	Mailing houses, call centers, and credit-monitoring providers carry minimum engagement sizes. Small populations pay close to the floor price regardless.
No in-house response	An enterprise has a security team, inside counsel, and a communications staff on payroll. A small firm assembles all of it mid-crisis at crisis rates — while the owners run the response instead of the business.
Cash flow	Forensics and counsel invoice in weeks. Insurance reimburses later, after retentions and within sub-limits. An enterprise absorbs the gap across quarters; a small firm covers it from operating cash.
Concentration	A smaller firm is usually one location, one practice, a short client list. Downtime stops all revenue at once, and losing a few anchor clients after the incident is not a rounding error.

A NOTE ON SMB BREACH STATISTICS YOU SEE ELSEWHERE

Precise-sounding small-business breach figures circulate widely in vendor marketing, often without a checkable source. Before you put any such number in a board deck or an insurance application, find the underlying study and confirm the year, the sample, and the definition of "cost." If you cannot, leave it out — exactly as this report does.

03 — WHAT REDUCES COST

The factors that measurably move the number

The same IBM study measures which factors raise or lower breach cost. Two findings matter more than the rest: how fast you contain, and how much of your detection and response runs without waiting on a person.

$3.61M	$5.49M	−$1.9M
Average cost when contained in under 200 days	Average cost when containment takes over 200 days	Average cost with extensive security AI and automation
IBM 2025	IBM 2025	IBM 2025

Breaches contained in under 200 days averaged $3.61M, against $5.49M when containment ran longer than 200 days. IBM Cost of a Data Breach Report 2025 Containment speed is the single largest lever a firm controls. Organizations with extensive security AI and automation saw average breach costs $1.9M lower and lifecycles roughly 80 days shorter. IBM Cost of a Data Breach Report 2025 In practice "automation" means detection and response that acts on a signal immediately — isolating a machine, killing a session — rather than queuing it for the morning.

What you are defending against

The threat data points at the same handful of controls. Ransomware was present in 44% of breaches, up 37% year over year. Verizon DBIR 2025 The human element was involved in 60% of breaches. Verizon DBIR 2025 Third-party involvement doubled to 30% of breaches. Verizon DBIR 2025 "Over 90% of successful cyber-attacks start with a phishing email." CISA The losses are not abstract: $16.6B in cybercrime losses was reported in 2024 — a record, up 33% year over year — with business email compromise alone accounting for $2.77B across 21,442 complaints. FBI IC3 2024 Internet Crime Report

Translating the findings into controls a smaller firm can run

CONTROL	COST DRIVER IT ADDRESSES	WHY IT MOVES THE NUMBER
EDR with around-the-clock monitoring	Containment speed	Most of the 241-day mean lifecycle is dwell time — the attacker operating unnoticed. IBM Cost of a Data Breach Report 2025 Endpoint detection that someone actually watches, at night and on weekends, is what separates the under-200-day outcomes from the rest.
Tested incident response plan	Lifecycle length	The first day of a breach should execute decisions, not make them. Knowing who calls the carrier, who engages counsel, and what gets isolated first removes the most expensive delays.

Offline or immutable backups	Ransomware — present in 44% of breaches Verizon DBIR 2025	A copy the attacker cannot encrypt or delete removes the extortion leverage. You restore on your schedule instead of negotiating on theirs. Test the restore, not just the backup job.
MFA on every account	Human element — 60% of breaches Verizon DBIR 2025	Phishing harvests passwords; MFA makes a harvested password insufficient on its own. Cover email, VPN, remote access, and admin accounts first — exceptions are where incidents start.
Vendor access review	Third party — 30% of breaches Verizon DBIR 2025	Inventory every vendor with access to your systems or data, restrict each to the minimum needed, and remove access the day an engagement ends. Your breach can begin on someone else's network.

A CAVEAT ON THE AUTOMATION FINDING

IBM's automation figures are measured across organizations of all sizes, mostly enterprises with in-house security operations. A smaller firm rarely builds that capability internally; it typically obtains the same effect — monitored detection that responds immediately — through a managed provider. The mechanism matters less than the outcome: signals acted on in minutes, not discovered in months.

04 — COST AVOIDANCE ROI

A framework for justifying the spend

Security spending competes with hiring, marketing, and rent. The honest way to evaluate it is expected loss — not fear, and not a vendor's slide. The framework is simple enough to do on one page.

The expected-loss formula

Expected annual loss = annual likelihood of a breach × expected impact if it happens. Both inputs are estimates. That is fine — the purpose is not prediction, it is comparing options on a consistent basis. Likelihood comes from your incident history, your industry's threat picture (Section 03), and how exposed your current controls leave you. Impact comes from the fixed-cost inventory in Section 02 plus your own downtime arithmetic: revenue per day of outage, times the days a realistic incident would cost you.

Controls work on both factors. MFA and email security reduce the likelihood that an attempt becomes an incident. EDR with monitoring, a tested response plan, and clean backups reduce the impact when one does — that is the under-200-day difference from Section 03 in your own ledger.

The insurance effect

Cyber insurance applications now ask specifically about MFA coverage, endpoint detection, backup isolation and testing, and offboarding discipline. The answers shape your premium, your retention, your sub-limits, and whether some markets will quote you at all. The direction is consistent — stronger controls buy better terms and more options — but the size of the effect varies by carrier, year, and book, so put no percentage on it until your broker quotes one in writing.

Worked example

> **HYPOTHETICAL — ILLUSTRATION ONLY**
>
> Every number in the table below is invented to demonstrate the arithmetic. None of it is a benchmark, a quote, or a statistic. Replace the middle column with your own estimates in the right-hand column, and pressure-test them with your broker and counsel.

LINE	HYPOTHETICAL INPUTS	YOUR FIRM
A. Annual likelihood of a serious incident (current controls)	10%	
B. Estimated impact if it happens (forensics, counsel, notification, downtime, attrition)	$600,000	
C. Expected annual loss (A × B)	$60,000	
D. Likelihood after the control set (MFA, EDR + monitoring, tested IR plan, isolated backups)	5%	
E. Impact after the control set (faster containment, clean restore)	$400,000	

F. Expected annual loss after controls (D × E)	$20,000
G. Reduction in expected loss (C − F)	$40,000
H. Annual cost of the control set	$30,000
I. Net expected benefit (G − H)	$10,000

Insurance effects — premium, retention, insurability — sit outside this math and accrue on top of line I. So does everything a spreadsheet cannot price: regulator goodwill, client trust, and the partner hours a long incident consumes.

Prepared by _____

Date _____

Reviewed with broker / counsel on _____

> **THE LIMIT OF EXPECTED-LOSS MATH**
>
> Expected loss averages over many years. A firm does not get many years if a single bad year is fatal — and Section 02 explains why the bad year hits smaller firms hardest. That tail risk is the case for insurance and for containment speed, even when the annual arithmetic looks marginal.

ELEVATE
SOLUTIONS

Elevate Solutions provides managed IT and cybersecurity for businesses that answer to regulators, clients, and courts.

Elevate Solutions

6230 Wilshire Blvd Suite 2120, Los Angeles CA 90048

(424) 400-6625 · support@elevatesolutions.io · elevatesolutions.io