CYBERSECURITY RISK BRIEF

The Cost of Inaction

Why Delaying Cybersecurity Investment Is Your Most Expensive Decision

$4.44M Global avg. cost per breach (2025)	**$10.22M** Avg. cost per breach in the US alone	**241 Days** Mean time to identify and contain

The Uncomfortable Truth

Every organisation believes a breach will happen to someone else. The data tells a different story. IBM's 2025 Cost of a Data Breach Report, spanning 600 organisations across 17 industries, confirms that the financial, operational, and reputational damage from cybersecurity failures is not a hypothetical risk - it is a statistical certainty for unprepared businesses.

The global average cost of a breach now stands at $4.44 million. In the United States, that figure has surged to a record $10.22 million, driven by escalating regulatory fines and extended remediation timelines. Healthcare organisations face average costs of $7.42 million per incident, while financial services firms absorb roughly $6.08 million. These are not outlier figures; they represent the new baseline.

Where the Money Goes

Breach costs are not a single line item. They compound across every function of your business:

Detection & Escalation	$1.47M avg. - forensic investigation, crisis triage, internal mobilisation. This is the largest single cost driver for the fourth consecutive year.
Lost Business	$1.38M avg. - operational downtime, customer churn, revenue loss during recovery. 80% of consumers say they would abandon a brand after a breach.
Post-Breach Response	$1.20M avg. - credit monitoring, helpdesk scaling, legal settlements, and compliance remediation.
Notification	$390K avg. - regulatory disclosure obligations, customer communications, and third-party coordination.

Regulatory Fines	$2.9B+ in GDPR and related fines globally in H1 2025 alone. Individual penalties routinely reach eight figures.

Beyond the Balance Sheet

Stock price impact: Publicly traded companies that suffer a major breach see an average stock decline of 5.7% within 30 days. Financial firms fare worse at 7.5%.

Recovery timeline: Nearly two-thirds of breached organisations report they are still recovering. Most take over 100 days to reach full operational restoration.

Customer trust: 46% of affected enterprises experience measurable drops in customer trust. In financial services, 38% of customers say they would switch providers after a breach.

SMB survival: 75% of small and mid-sized businesses say they would not survive more than three weeks after a severe attack. Average downtime is 21 days.

The Threat Landscape in 2025

The attack surface is expanding faster than most security programmes can adapt. Phishing remains the most common breach vector at 16% of incidents, costing an average of $4.8 million per event. Supply chain compromises account for nearly 15% of breaches, and ransomware features in 44% of all incidents analysed by Verizon.

AI is accelerating both sides of the equation. Attackers are using generative AI in 16% of breaches, primarily for phishing and deepfake impersonation. AI-generated phishing emails now achieve a 68% open rate - nearly double that of conventional campaigns. Meanwhile, shadow AI (unsanctioned AI tools used by employees) was involved in 20% of breaches, adding an average of $670,000 to incident costs.

THE INACTION EQUATION

A $500K annual investment in data protection, incident response planning, and security automation typically saves $1.9M per breach event. The average organisation faces a 27.7% probability of experiencing a material breach within any two-year window. Doing nothing is not cost-neutral - it is the most expensive option on the table.

What the Data Proves Works

Not all organisations pay the same price. IBM’s research identifies clear differentiators between those who contain costs and those who don’t:

AI & Automation in Security $1.9M saved per breach. 80-day reduction in breach lifecycle.	**Incident Response Planning** $1.23M saved per breach. Organisations with tested IR plans contain incidents weeks faster.
Encryption & Data Protection $360K saved per breach. Tokenisation and encryption reduce the value of stolen data to zero.	**Employee Training & MFA** Human error drives 95% of breaches. Credential-based attacks rose 71% YoY.

The Board-Level Question

This is no longer an IT decision. It is a business survival calculation. Every day without adequate protection adds to your cumulative risk exposure - the Annual Loss Expectancy that compounds with each quarter of inaction.

The organisations that thrive through this threat landscape are not those with the biggest budgets. They are the ones that treat data protection as a business enabler, not a cost centre.

Use our interactive Cost of Inaction Calculator to model your organisation’s specific financial exposure based on revenue, industry, data sensitivity, and existing controls. Quantify the gap between where you are and where you need to be.

Sources: IBM Cost of a Data Breach Report 2025 • Verizon 2025 Data Breach Investigations Report • SQ Magazine Cyber Threat Statistics 2025 • Ponemon Institute • PKWARE Financial Services Breach Analysis