

The Growing Cost of Data Loss

Your Data Has Value — And Losing Control of It Has a Measurable Cost

Protecting digital information is no longer simply an information-technology issue. Data breaches, ransomware, theft of intellectual property, compromised credentials, and unauthorized access to confidential information impose measurable financial costs on individuals and organizations.

The numbers show both the **size of the problem and how rapidly the cost is increasing**.

According to IBM's **2026 Cost of a Data Breach Report**, the average data breach now costs an organization **\$4.99 million globally**, a **12% increase in a single year and the highest global average IBM has recorded**.

The cost in the United States is substantially higher. IBM reports an average U.S. data-breach cost of approximately **\$11.5 million**.

Some industries experience particularly high losses. In 2026, IBM reports an average breach cost of **\$6.64 million for healthcare**, the highest industry average for the 15th consecutive year. Financial-services breaches averaged approximately **\$6.3 million**, while energy-sector breaches averaged approximately **\$5.2 million**.

The problem is not limited to large corporations.

The FBI's **2025 Internet Crime Report** recorded **1,008,597 complaints** from the American public—up from **859,532 in 2024**. Reported losses from cyber-enabled crime approached **\$21 billion** during 2025 alone.

The threat itself is also expanding. Verizon's **2026 Data Breach Investigations Report** examined more than **31,000 real-world security incidents and more than 22,000 confirmed data breaches across 145 countries**—the largest number of breaches Verizon has examined in a single annual report.

Ransomware was involved in **48% of the breaches** analyzed by Verizon.

Organizations Are Spending Billions to Protect Their Information

The amount being spent on information security provides another measure of the value organizations place on protecting their data.

Gartner reported worldwide information-security spending of approximately:

2024 — \$193.4 billion

2025 — \$213.0 billion

2026 — approximately \$240 billion

That represents an increase of approximately **\$46 billion in annual security spending in only two years.**

Security software alone is projected to increase from approximately **\$95.0 billion in 2024 to \$121.2 billion in 2026**, while spending on security services is projected to rise from approximately **\$77.1 billion to \$92.8 billion.**

These expenditures demonstrate that protecting digital information has become a major and continuing investment for organizations worldwide.

Encryption Is Part of the Protection

Despite the enormous financial investment in cybersecurity, encryption gaps remain.

IBM's 2026 research found that only **37% of breached organizations encrypted sensitive data both at rest and in transit**, and only **34% had visibility into their cryptographic assets.**

Encryption cannot prevent every cyberattack, system failure, theft, or human mistake. What it can do is provide another critical layer of protection for the **data itself.**

That is the role STIKABA is designed to address.

STIKABA provides **Unconditional Data Security** through its implementation of One-Time Pad encryption, combined with controlled Key generation, distribution, management, access, and use.

The objective is straightforward:

Your data has value. Protect the data—not just the computer, network, or account that contains it.

STIKABA — Unconditional Data Security