The ROI of a Modern Privacy Program

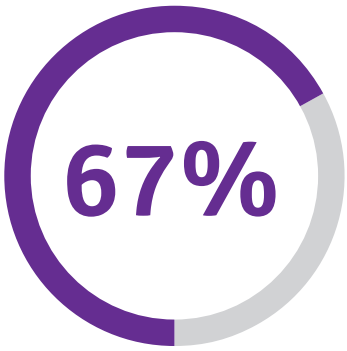
Table of contents

Introduction

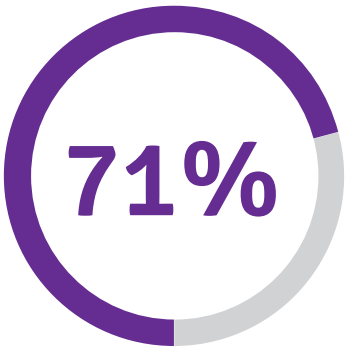
For every $1 an organization invests in privacy spending, it receives an average $2.70 return on investment, according to a 2020 Cisco study that asked privacy professionals across various industries in 13 countries to estimate their privacy investments' financial benefits.

The same study finds that 47% of organizations report a return that more than doubles their privacy spend, and over 70% show "significant" business benefits — up from 40% in 2019.

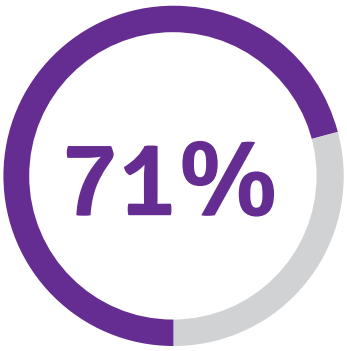
Those organizations see concrete business outcomes from their privacy programs across all areas of business. For example:



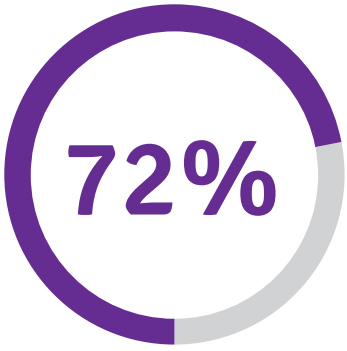
report a reduction in sales delays



show fewer and less costly data breaches

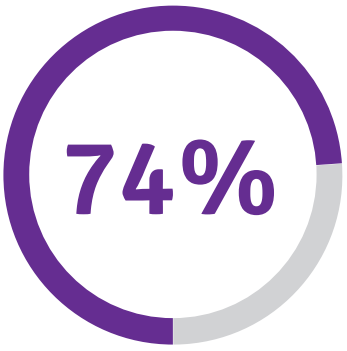


reveal improved agility and innovation



achieve greater operational efficiency

find their company more attractive to investors



reveal improved customer loyalty and trust

The takeaway? ROI on privacy investments are both concrete and calculable.

For every $1 an organization invests in privacy spending, it receives an average $2.70 return on investment, according to a 2020 Cisco study.

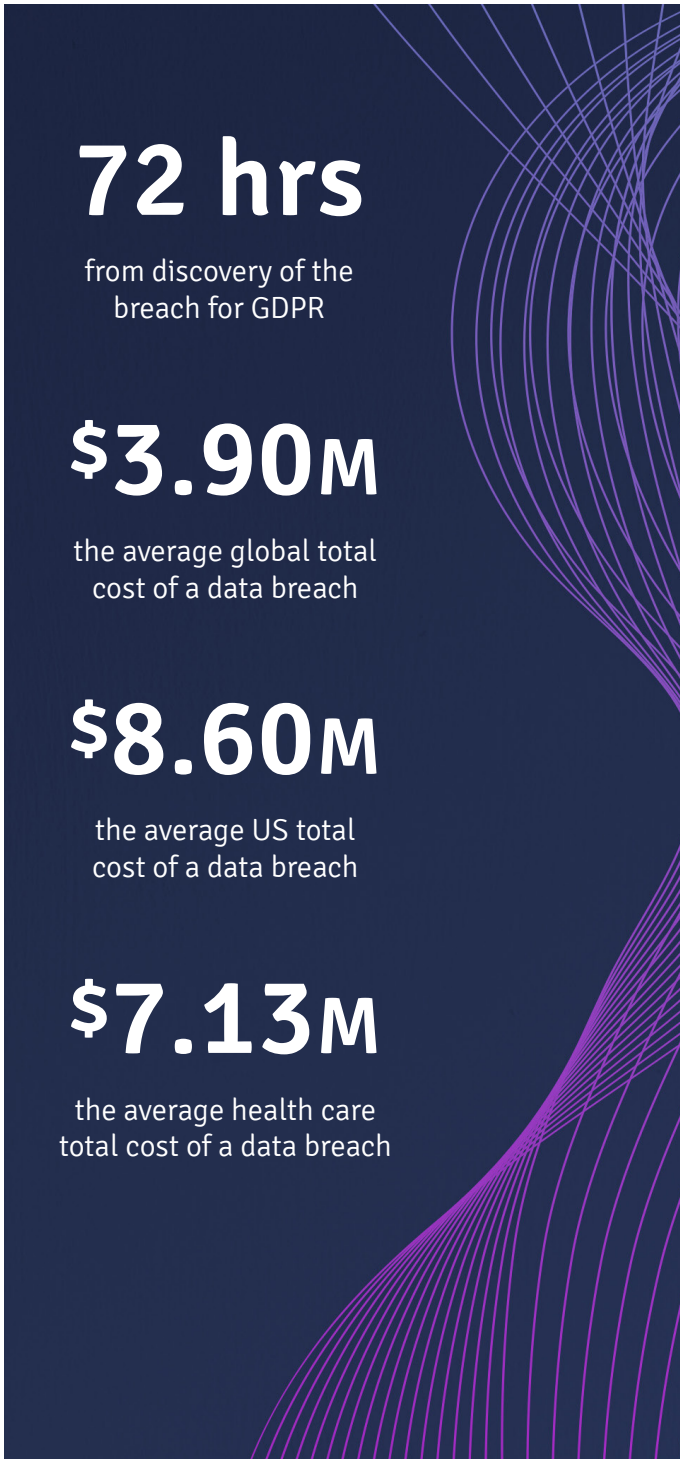
The Return on Breach Response

Establishing and operationalizing a modern privacy framework enables organizations to react quickly to breach incidents, track and identify where a breach comes from, and respond to regulating authorities within the required timeframes (e.g., 72 hours from discovery of the breach for GDPR, for example).

According to IBM, the average global total cost of a data breach is around $3.90 million — and has grown in recent years. Those averages vary by country — climbing as high as $8.6 million in the U.S. — and industry, where health care carries the steepest risk of $7.13 million. On average, companies facing a breach incident incur about a $150 price tag per record.

Organizations with high accountability — meaning they've met specific standards for effective compliance and protection of individuals' data — are over twice as likely to avoid data breaches as companies who have low accountability.

When data breaches do inevitably occur, businesses with high accountability report lower costs and fewer negative outcomes from these incidents — with 19% less downtime, 28% fewer impacted records, and 10% lower costs.



The Popularity of Privacy

An increasing number of forward-looking companies are taking the plunge and strategically building their privacy frameworks.

Frameworks like the **NIST** (created by the National Institute of Standards and Technology) and the **ISO/IEC 27701:2019** (a privacy extension designed to enhance the existing **ISO/IEC 27001** for information security) create standardized, common practices that companies can use to enhance privacy and reduce risk.

Seventy-four percent (74%) of organizations are putting spend behind maturing their privacy frameworks in the areas of policies and procedures, risk assessment, leadership and oversight, response and enforcement, monitoring and verification, training and awareness, and transparency.

Seventy-four percent (74%) of organizations are putting spend behind maturing their privacy frameworks.

These efforts include:

- incorporating privacy by design into the development of products and services
- expanding privacy teams and building privacy programs
- building cross-functional collaboration among privacy, security, and governance teams
- proactively informing and educating consumers about how their data is used
- investing in data privacy technology

The Competitive Advantage of a Privacy Framework

For a competitive advantage, some organizations — particularly those that function as vendors — seek certifications for Cross-Border Privacy Rules and international data transfers. **These certifications serve to validate sound privacy practices and can make a vendor more appealing to a buyer.**

Investors also keep an eye on privacy compliance and good data practices in evaluating the risk and reward of taking on a company as a new venture or acquisition.

Companies that are merging, for example, must consolidate a tremendous amount of data that may be sensitive, personal, or regulated — a time-consuming and costly effort under the best of circumstances. Privacy-compliant companies that adopt responsible data practices require less integration lift and carry less data risk for potential buyers — a quantifiable selling point.

Privacy-compliant companies that adopt responsible data practices require less integration lift and carry less data risk for potential buyers — a quantifiable selling point.

Brand Trust and ROI: Customers Are Paying Attention

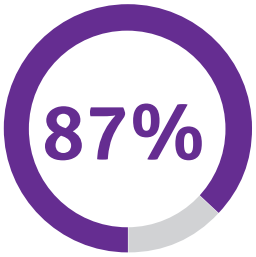
Data privacy and protection regulations focused on data subjects' rights have given individuals the legal right to request and access the information that companies collect and process about them — and hold those companies accountable for how they do it.

These regulations have also raised general awareness about data privacy rights. Around 60% of European consumers now know that regulations exist to protect their data — up from 40% five years ago.

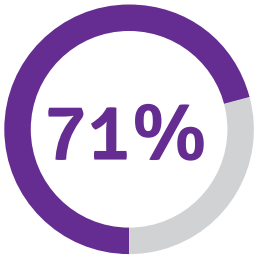
60% of European consumers now know that regulations exist to protect their data

40% of European consumers five years ago know that regulations exist to protect their data

Highly publicized data breaches have also contributed to data security concerns among customers. A report by McKinsey and Company shows that 87% of customers would not do business with a company they suspected of inadequate security practices — and 71% report that they would stop doing business with an organization that gave away sensitive data.



of customers would not do business with a company they suspected of inadequate security practices



of customers would stop doing business with an organization that gave away sensitive data

While data breaches are responsible for a good deal of damaged customer trust, not all is lost in the event of a breach. The report shows that 50% of respondents are more likely to trust companies that act quickly on a breach incident and disclose it to customers.

50% of respondents are more likely to trust companies that act quickly on a breach incident and disclose it to customers.

Additionally, respondents to the McKinsey report put the greatest trust in industries that collect and process sensitive data in order to provide a product or service — like financial and health care— compared to consumer packaged goods, media, or entertainment companies.

Enhancing customer trust fosters a positive customer experience — and a positive customer experience can increase sales, having a beneficial impact on ROI.

Enhancing customer trust fosters a positive customer experience — and a positive customer experience can increase sales, having a beneficial impact on ROI.

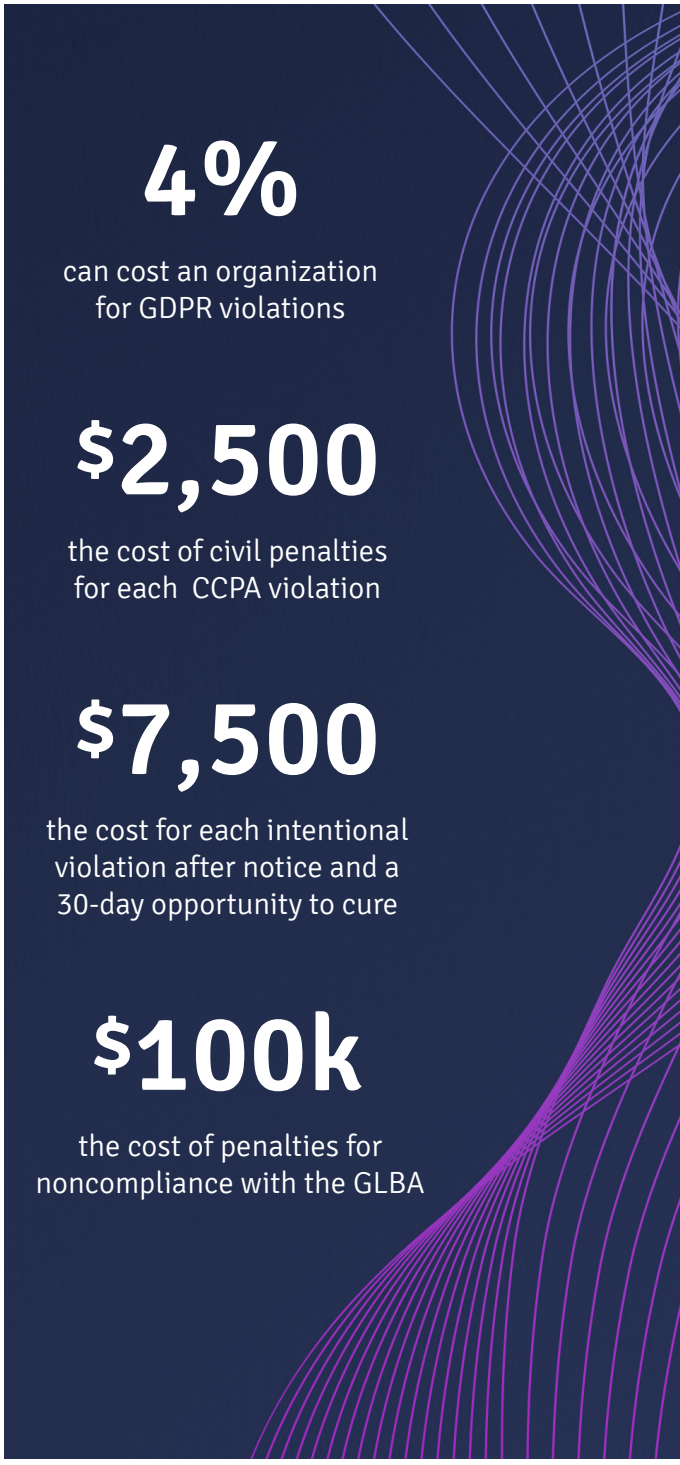
Regulatory Compliance: You Can't Afford Not To

Failure to comply with multiple and varied privacy and protection regulations can result in steep fines for companies.

GDPR violations can cost an organization up to 4% of its global revenue, and LGDP fines can cost up to 2% of a company's Brazilian revenue — along with other penalties like publication of the violation, the temporary suspension of the right to use personal or sensitive data, and suspension of business activities.

CCPA violations can bring civil penalties of $2,500 for each violation — or $7,500 for each intentional violation after notice and a 30-day opportunity to cure.

Noncompliance with the Gramm-Leach-Bliley Act (GLBA), which regulates finance organizations, can result in penalties of up to $100,000 for each violation. Individuals can also face the same fines — plus possible prison time of up to five years.




Failure to comply with multiple
and varied privacy and protection
regulations can result in
steep fines for companies.

What a Modern Privacy Program Looks Like

To avoid hefty noncompliance fees, expensive data breaches, reputational loss, and other costly liabilities, **companies need to invest in data privacy technology that incorporates privacy by design and supports their privacy framework.**

Start with deep data discovery to map, inventory, and categorize all sensitive, critical, regulated, and personal data — across the organization. By having all enterprise data in one place, organizations can take action on their data with privacy apps that automate end-to-end data subjects rights requests, document third-party data sharing, manage policy-driven data retention, and more.

Start with deep data discovery to map, inventory, and categorize all sensitive, critical, regulated, and personal data — across the organization.

Schedule a BigID demo to learn more about how your organization can maximize the ROI of a modern privacy program.