IBM **Security**

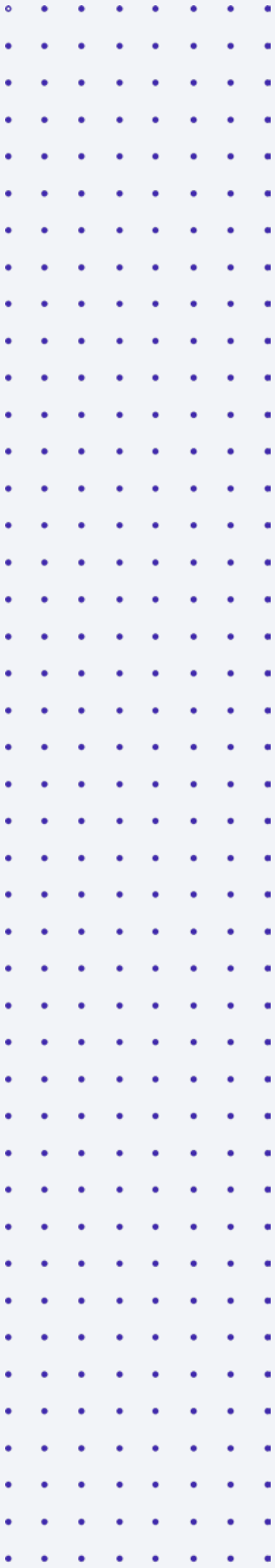
August 2019

Why data privacy matters

Build trust to help build your business

IBM

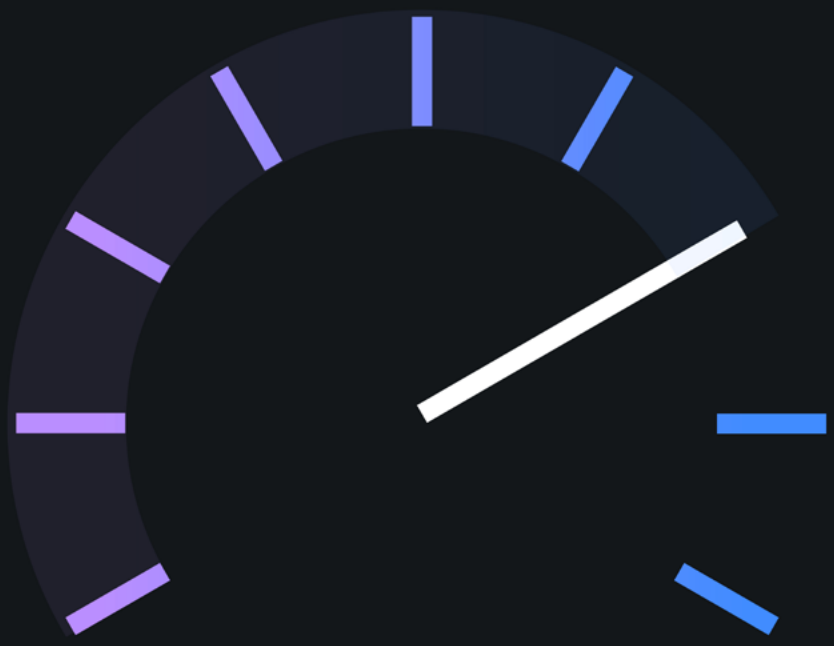
Contents



Psst ... Privacy is more important than you realize

The idea of privacy protection isn't something new. It has, however, become a lot more complicated since the advent of global markets and digital technologies. **Today, privacy extends to a wide range of personal data and information that may be stored on personal digital devices, in corporate data centers and even in the cloud.** Compounding that complexity are ever-changing consumer views of privacy, industry regulations and even geopolitical guidelines — all of which need to be aligned and adhered to as companies look to avoid the penalties of getting privacy wrong, from heavy fines to angry customers.

If penalties for non-compliance and customer defection represent the punitive side of privacy, there's also a positive side — namely, that customers are more likely to do business, and may even do *more* business, with companies they trust. Put another way, privacy isn't simply a must-do mandate, but an important part of your business strategy that can do a lot to help boost your brand and your bottom line. In this ebook, we'll explore how building trust can help you build your business in a privacy-conscious world and focus on the principles that form the foundation of a sound privacy strategy.



Privacy is an important part of your business strategy that can help boost your brand and your bottom line.

With the right strategy, privacy may not cost you agility

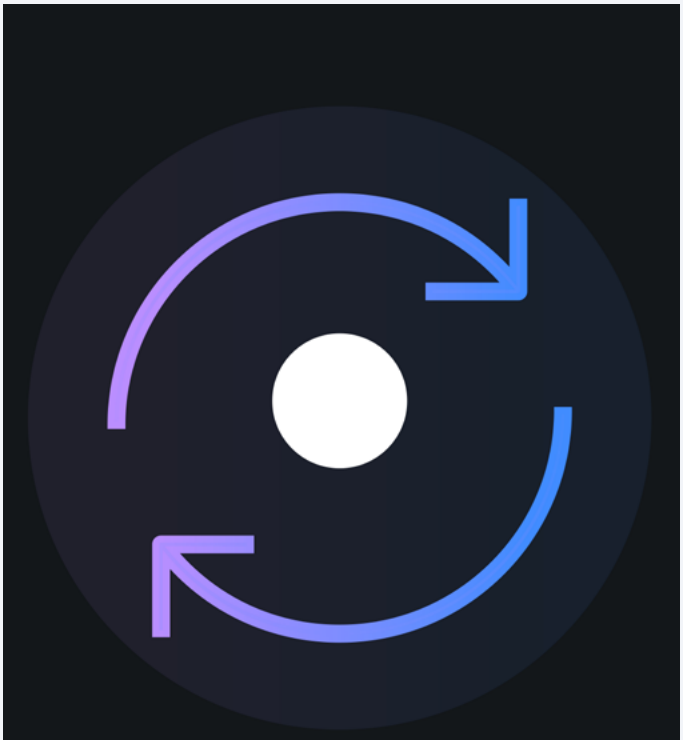
Sometimes privacy compliance highlights the animal tendencies of a business. Some businesses, like turtles, may be slow to adopt new compliance measures. Others, like ostriches, may hide their heads in the sand and ignore them. Still others may believe they can outfox regulators with partial compliance. But companies that don't take compliance seriously could face serious consequences. New geographic pressures on privacy — such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) — have the power to levy substantial fines and disrupt business.

The question on the mind of companies should not be how do we get around compliance, but rather how do we align compliance with our business roadmap? This question, in turn, should lead to a broader discussion that answers:

- Where are the synergies and/or efficiencies in the data security measures we're taking today and the privacy security measures we'll need to take tomorrow?
- How do we adapt to new regulatory requirements and growing pressure from consumers to make privacy transparent?
- What actions will lead us to being recognized as a privacy leader in our industry?
- How do we leverage our privacy practices to drive better business results?

The new reality is that businesses need to look forward to the role that privacy can play in helping build brand equity and better customer relationships. This approach to privacy can be summed up in three important steps:

1. Start building a strong privacy program today.
2. Use privacy intelligence as you would other data intelligence: to uncover actionable insights that can help improve your business and build trust with consumers.
3. Automate your privacy controls to reduce errors and increase cost efficiencies.



78 percent of consumers surveyed say it is 'extremely important' that companies quickly take the right actions to stop a data breach.[1]

Start building a strong data privacy program today

The first step toward a strong data privacy compliance program begins when you stop seeing privacy as a security problem and start seeing it as a strategic advantage. Privacy isn't a security box to be checked off, but a continuous part of the checks and balances that comprise all your business processes. How can you try to build privacy and security into every new product or process? Follow these tips to help build a foundation for your security strategy:

Step 1: Do some serious security soul-searching
If your privacy program has holes, don't hide them; find them. Do a thorough and honest assessment of the privacy controls you currently have in place, including a privacy impact assessment highlighting the risks you face right now, and use this as the starting point in building a readiness roadmap.

Step 2: Look for the big picture
Typically, privacy data is pervasive; it doesn't live on an island but is interspersed throughout your organization. Businesses therefore should consider implementing privacy measures that extend data discovery, visibility and protection across the entire organization.

Step 3: Start at the top with executive buy-in
Seek executive support for your security strategy. If executives see the value of privacy, they can help find the budget to support it. Privacy also should become a part of the corporate culture, and culture can be a top-down initiative. If privacy isn't important to the CEO, it most likely will not be important to mid-level management.

Step 4: Consider compliance a moving target
Privacy rules and requirements are constantly changing and evolving. As soon as you're compliant, you might be at risk of falling out of compliance if there's a shift in the regulations. That's why it's important that businesses view their privacy strategy as an ongoing journey: get where you need to be today to achieve compliance, and be prepared to move tomorrow as new privacy changes are introduced.

Data privacy is the new strategic priority
As firms face a growing list of data protection regulations and customers become more knowledgeable about their privacy rights, developing a data privacy competence has never been more important. This new commissioned study conducted by Forrester Consulting evaluates the state of enterprises' data privacy compliance in a shifting regulatory landscape.

→ Read more

Organizations with well-rounded strategies that commit to data privacy for more than just compliance stand to realize a number of benefits, including enhanced customer trust.[2]

View privacy intelligence as business intelligence

Privacy leaders do more than simply react the fastest to new requirements. They proactively look for ways to leverage privacy to enhance customer relationships and improve business outcomes. **By giving privacy intelligence the same value as other business intelligence, companies can uncover actionable insights to help them develop effective privacy strategies.**

Tips for creating a privacy strategy:

- Create a unified view of data security and privacy that extends across your data platforms as well as cloud computing platforms;
- Manage employee, partner and customer access to personally identifiable data;
- Develop enforceable data security and policy rules that promote secure data storage, data disposal and all data touchpoints;
- Identify actionable risk mitigation procedures and prioritize them in preparation for privacy incidents that may occur.

What's the privacy payoff? Data-driven privacy insights can help you develop pro-privacy processes and policies to address compliance and promote growth.

A privacy program can help you address the privacy requirements of international regulations. Learn how a common set of principles around transparency can help your organization address those requirements.

→ Read the blog post

Automate your privacy controls

It only takes a moment to make a mistake, but even a moment can be too much in a world where personal data moves at the speed of microseconds. **With automated privacy controls, businesses can help protect personal data, whether at rest or in motion, before mistakes can happen.** Automation alone, however, may not protect your data unless you have privacy policies in place, such as:

- Combine encryption and monitoring in a way that can help protect personally identifiable data wherever it is: at rest, in motion, on premises or in the cloud.
- Automate auditing reports and regulatory requests for documents to help streamline the process and eliminate "fire drill" responses.
- Use automated identity controls to help manage data access in a secured, consistent manner.
- Have automated, orchestrated data privacy security responses at the ready to help you deal with data security and privacy incidents or breaches when they occur.

What's the privacy payoff? Automated, orchestrated privacy controls can help reduce the very real risk of manual errors, reduce operational complexity and improve your response times to critical privacy and security issues.

Privacy: The bottom line

Privacy isn't just an important part of your IT security posture. It's an integral part of your corporate DNA. It can help define your brand, determine your customer relationships and may ultimately drive your bottom line. In the future, digital privacy may play an increasingly important role for consumers as well as the government agencies that are entrusted with protecting them.

It's no secret that many businesses today struggle to navigate an increasingly complex landscape of changing privacy regulations and shifting consumer sentiment. But businesses don't have to face privacy issues alone. IBM can help — with our people, our products and our experience.

Build a data privacy program

Implement a dynamic privacy foundation.

- IBM Security Data Privacy Services
- IBM Promontory

Gain privacy insights

Increase visibility into risks and use privacy insights to help generate business impact.

- IBM Security Guardium Insights
- IBM Security Data Risk Manager
- IBM Security Cloud Identity
- IBM Security Resilient

Automate privacy controls

Help protect personal data at rest and in motion, on premises and in the cloud.

- IBM Security Guardium Data Protection
- IBM Security Data Privacy Services
- IBM Promontory

Sources

1. IBM Cybersecurity and Privacy Research, conducted by The Harris Insights & Analytics, on behalf of IBM, April 13, 2018.

2. Data Privacy Is The New Strategic Priority, Forrester Opportunity Snapshot: A Custom Study Commissioned by IBM, JULY 2019

IBM **Security**

© Copyright IBM Corporation 2019

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
May 2019
All Rights Reserved

IBM, the IBM logo and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

Please Recycle

57025957USEN