



SECURITY

Data Privacy and Data Security: What's the Difference?

While data privacy and data security are related, they should be addressed in different--but integrated--ways.

[Karen D. Schwartz](#) | May 02, 2019



Companies live with constant fear of experiencing a data breach because they understand the harm it can cause—not only to their reputation, but to their bottom

confidentiality, integrity and availability. Data privacy revolves around the use and governance of personal data. This can include everything from personally identifiable information (PII) to financial information, to information about a person's career, education, health, family or criminal history.

From these definitions, it's clear that these two terms—“[data security](#)” and “data privacy”—should not be used interchangeably. While they are certainly related and are both extremely important, they should be addressed in different, but integrated ways.

That integration is critical, but complicated.

“We like to say you can have security without privacy, but you can't have privacy without security,” says Cindy Compert, CTO Data Security and Privacy for IBM Security. “Consider data that you consider to be solidly secured: It's encrypted, access is restricted, and you have put in place multiple overlapping monitoring systems. In all meaningful senses of the word, the data is secure. But when you add privacy into the mix, it becomes a little more convoluted. For example, while the customer service agent may be provisioned to access your account details after going over some security questions, privacy won't allow the same individual to check the account of a family member, even though they have access privileges to that information.”

The Growing Importance—and Complexity—of Data Privacy

Increasingly stringent regulations in the United States and abroad have put [data privacy](#) concerns and compliance front-and-center for most companies. For example, privacy regulations in laws like the Health Insurance Portability and Accountability Act (HIPAA) and the Children's Online Privacy Protection Rule

Union is even broader, defining a privacy violation as the illegal retrieval or disclosure of “any information relating to an identified or identifiable natural person.” That information can include posts on social media, email addresses, bank details, photos and IP addresses.

Failure to comply with this regulation can result in fines of up to 4% of gross revenue.

Each organization defines its own data privacy policies, which typically include what data will be collected, how that data will be collected and used, who will have access to it, whether or how data can be shared with third parties, if data can be legally collected or stored, and how long data will be stored. They also detail which regulatory restrictions the organization must comply with.

This information is critical, not only to companies hoping to avoid fines and other penalties, but to customers themselves. According to a recent [report](#) from RSA, data privacy concerns are sky-high right now. The report found that 80% of respondents consider financial and banking information the top concern, while 72% consider personal identity information a significant area of concern. More than half of millennials are concerned with personal information being used for blackmail. A [Harris Poll](#) last year sponsored by IBM backed this up, finding that three-quarters of global consumers would not buy a product or service from a company if they didn't trust that company to protect their data.

Clearly, failure to take data privacy seriously can have serious consequences for companies themselves. According to a [report](#) from Cisco, two-thirds of companies say they are seeing sales delays due to data privacy questions from their customers.

“Basically, good privacy is good for business,” says Robert Waitman, director of

balancing act. For one thing, they sometimes require different tools or approaches. Popular types of data privacy tools include browser extensions and add-ons, password managers, private browsers and email services, encrypted messaging, private search engines, web proxies, file encryption software, and ad and tracker blockers. [Data security](#) tools include identity and access management, data loss prevention (DLP), anti-malware and anti-virus, security information and event management (SIEM) and data masking software.

But there are certainly technologies that can do double duty, providing some level of both data security and data privacy protection. These include virtual private networks (VPNs), key management, real-time monitoring software, attribute-based access control (a more granular level of control than role-based access control), and customer identity and access management (CIAM). Most experts recommend a mix of all of these technologies.

“The companies that are doing it right have a unified program, with an agreed-upon classification framework, along with an assessment process and controls based on the sensitivity of the data,” Compert says.

But it’s not that simple. To make matters even more complicated, not all data is created equally. In other words, some data is simply more sensitive than others, requiring different types of protection.

“Let’s say that your baseline for all personal data is encryption, but for highly sensitive data, you might add things like monitoring the privileged users who have access,” Compert says. “For example, you may choose to monitor all activity of a database administrator, creating an audit trail to make sure they are only accessing the data they need to access.”

Putting it All Together

Clearly, marrying data privacy and security into one comprehensive program isn't easy. For many, the GDPR framework has become a de facto privacy controls framework, because it lays everything out well.

“Going through the GDPR prep process or any privacy regulations can help organizations get their data privacy in order,” Waitman says. He noted that the Cisco report found that companies that have made the effort to prepare for GDPR are seeing shorter sales delays than those that haven't. They are also incurring less impact from data breaches when they occur.

“If you have your data house in order and know where your data is, how to protect it, and who has access to it, if something goes wrong and there is a breach, you have already done the right thing to control your data,” he says.

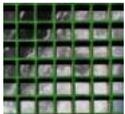
In addition to complying with regulations and keeping customers happy, there is another important reason to take the initiative: Data stores continue to grow, and much of that data is a privacy concern. According to [Gartner](#), the backup and archiving of personal data will represent the largest area of privacy risk for 70% of organizations by 2020.

While chief privacy officers, CIOs and the legal department certainly play a major role in this effort, IT professionals also have a role.

“A lot of privacy professionals don't understand the nature of technology that's available to help accelerate the process, like scanning of personal data,” Compert says. “If IT professionals take the time to educate themselves on data privacy and the regulations that apply to their organization, they will be able to team up with

0 COMMENTS

RELATED



Fertility Database Relies on Blockchain for Security

APR 05, 2019



Phishing Attacks Exploit Popularity of Netflix, AMEX

MAR 25, 2019



Prevent Getting Hacked With Ten Counterstrategies

MAR 09, 2019



City of Las Vegas Makes Bet on Advanced Threat Protection Solution

FEB 13, 2019

ITProToday™

an informa business

[About](#)

[Advertise](#)

[Contact Us](#)

[Sitemap](#)

[Ad Choices](#)

[Privacy Policy](#)

[Terms of Service](#)

[Cookie Policy](#)

Follow us:

