PwC's Governance Insights Center
November 2022

Trust, risk, and opportunity: overseeing a comprehensive data and privacy strategy

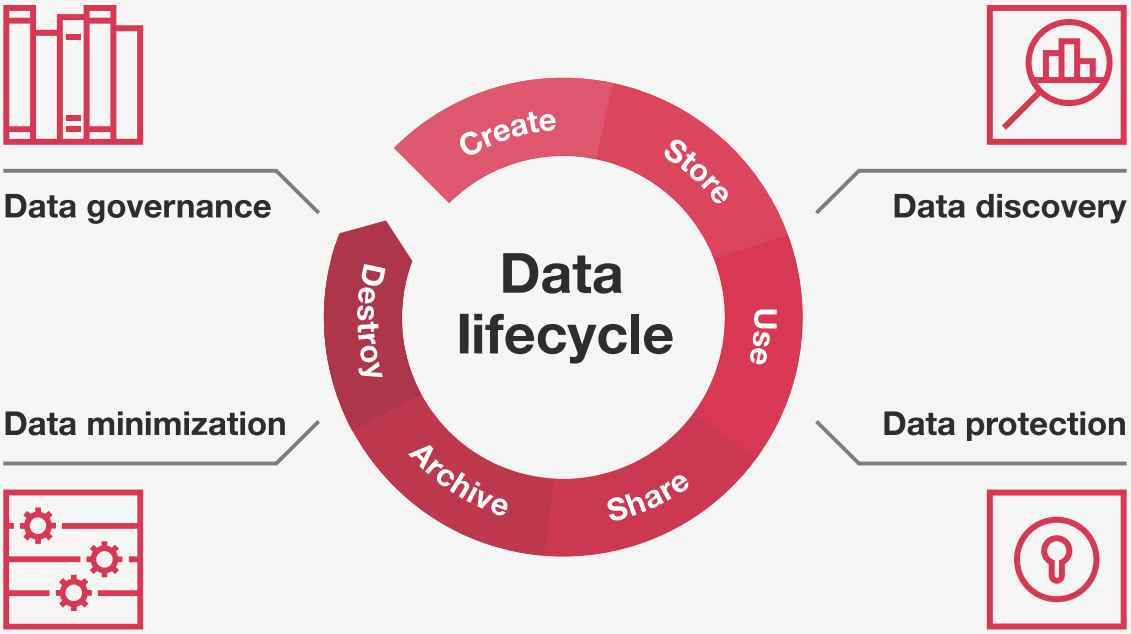
In today's world, data is power. The ability to collect and use vast amounts of data can give companies a competitive advantage. But with that opportunity comes risk and the duty to protect data privacy. Here's where boards come in.

pwc

Data is changing the competitive landscape. The volume of data now available to companies means they can find efficiencies, develop and target new products, gain customer insights, optimize operations, and tailor business strategies in ways they never could before, with a speed never thought possible. But collecting and using data also brings risk that it could be misused or accessed by threat actors. Converting data into value, securely and ethically, is the business imperative for the next decade.

The companies that most effectively take charge of their data throughout the data "lifecycle" will have the greatest opportunities for success. Given the opportunity and risk involved, it's essential that boards play a key role in the process.

Understanding the data lifecycle



- **Data discovery:** What types of data does our company collect? What data is most valuable? What data is most sensitive? How is the data used and is it used ethically?
- **Data protection:** What data is required to be protected? What other data should be protected? What processes are in place to offer that protection?
- **Data minimization:** What types of data are collected but not used? Do we have old data that is no longer used and can be eliminated? In what ways could our company's data collection (and risk) be minimized without losing current functionality or value?
- **Data governance:** Do we have the right people, processes and policies, and technology to govern our data and meet compliance and privacy requirements? How could they be improved?

Working through the data lifecycle, the board can dig deeper into the overall data strategy. When companies collect personal data from customers, employees, and others, they are expected to keep that data secure and protect its owners' privacy. Data privacy regulations, which are growing quickly, dictate some of this. But the individuals whose data is being collected are also keen to know what data companies are holding, why, and how it is being used.

Failing to protect this data leaves companies open to loss of consumer and employee trust. It can lead to brand damage, financial losses, and penalties and audits from regulators.

A company's future growth and ability to innovate depend on how well it uses and protects that data. As companies navigate their data and privacy strategy, boards will want to ensure that the company develops one that is holistic, creates trust with stakeholders, and manages related risks.

76%

of global consumers say that sharing their data with companies is a "necessary evil."

Source: PwC, *In data we trust: Living up to the credo of the 21st century*, September 2020.

Data discovery

Fundamentally, the question of how companies collect, use, and protect data is tied to the business strategy. For the board to make those connections, it starts with understanding what data the company collects, how it is stored, and how it is used.

To understand the business purpose and use of each element of data collected requires reporting from a team with cross-functional expertise in finance, lines of business, IT, marketing, HR, legal, data governance, data analytics, and data privacy. Some companies may have a Chief Information Officer (CIO), Chief Technology Officer (CTO), Chief Data Privacy Officer (CDPO), or another senior executive overseeing the data strategy. By leveraging this expertise, the board can evaluate the overall risk profile of the data strategy. Is the data collected and used in a legal and ethical manner? Do we have the data owner's consent? Is the data trustworthy and without biases?

While companies collect various types of data, the board and team will want to pay close attention to personal and sensitive data collected, which requires the most thorough data protection and compliance with data privacy regulations.

Pay extra attention to personal data

Personal data is information that relates to an identifiable person, either directly or indirectly, and requires data protection. Examples include: a name and surname, a home address, and email address.

Sensitive personal data is a subset of personal data and is defined as information that directly or indirectly reveals a person's race, ethnicity, political or philosophical views, religious beliefs, union affiliation, criminal record, or any data related to their health or sexual life. Holding this information usually requires additional safeguards. Examples include: a person's race or religion, health information, and biometric information.

Another important piece of the data discovery puzzle is the fact that individuals now have a growing ability to access and delete their user data as many global data privacy regulations give individuals this right.

Finally, an increasing challenge for companies that collect data is that many technology platforms are tightening restrictions on the use of cookies and online tracking, and greater transparency on privacy disclosures. All this is leading companies to rethink the information they gather and the ways it is collected.

Data protection

Data protection must be integrated into the company's cyber-risk management program. A data protection strategy should create and foster trust with stakeholders. It should involve continually training employees—especially those working remotely—on cybersecurity and privacy policies and practices. Good cyber and privacy hygiene should be enabled with technologies such as encryption, masking data, multi-factor authentication, and strong passwords.

Although most companies work to secure and protect the privacy of the data they collect, a surge in cybersecurity breaches illustrates the difficulty in doing so. Reportable data breaches, including those involving unauthorized disclosure of personal data, require timely disclosure based on various global cybersecurity and data privacy rules and regulations. These thefts may open the company up to reputational harm, financial costs, penalties, and loss of trust. With the growth in digitization, remote working, and sophistication of threat actors, the risk of data loss has increased.

Improving transparency - crafting a good external data privacy statement

Companies need to maintain an up-to-date external data privacy statement that discloses how the company uses, stores, and disposes of data, and how it obtains consent from consumers. Effective disclosure will provide details about collection, creation, use, transfer, storage, and deletion of personal data. It will detail whether the data was used for its stated purpose and provide privacy attestations from third parties. Most of all, it will ensure that customers and shareholders know how the company is protecting their information. These disclosures are often made to comply with global data privacy laws.

Where do boards come in? As management protects data, the board should engage in robust discussions about the adequacy of the protection and privacy program, including information on the effectiveness of controls and whether resources are sufficient. Boards will also want to make sure they are aware of key applicable cybersecurity and data privacy laws, and any major violations. Board reporting would include information about any reportable cybersecurity events, instances of non-compliance with privacy requirements, and how management is responding.

Navigating the patchwork of global privacy laws is challenging: 137 out of 194 countries worldwide have legislation to secure the protection and privacy of data. In the US, laws vary by state and there are more than 50 data privacy and protection bills in the works.

Source: United Nations Conference on Trade and Development

Data minimization

Once the board understands what data is collected and how it is protected, it can begin to explore with management whether any of that data could be minimized while still achieving the company's goals for the data. Almost any data can be a source of risk: from bad decisions and from malicious actors accessing sensitive information. Companies can minimize that risk by minimizing the target. They can protect the data they need, and only the data they need—eliminating the rest. Drafts, duplicates, superseded data, legacy data, and unnecessary employee personal data are common candidates for elimination.

A qualified cross-functional team can also report on ways to use fewer, more capable data repositories for better access and control—another way to eliminate targets and risk.

Data governance

The company's data governance will touch all of these areas: collecting, strategically using, protecting, and minimizing data. The board's role is to oversee management's governance of the data and ensure the people, processes, and technology in place are effective.

Some businesses set data controls by function, some by business line. But to really get the full value of data, a centralized data governance program can help reduce the risk of wrongful access and compliance errors, and unlock missed opportunities. The benefit of centralization cannot always be achieved, however. It is limited by the growing number of data localization laws and data transfer restrictions, which effectively create digital walls between countries. 60% of the world's population now lives in a territory where their data is either required to be stored locally or is subject to some form of cross-border data flow restriction. This means that US-based multinationals are no longer able to use their US-based talent, infrastructure, and controls and processes to support their global operations. They are required to set up these functions and activities in each country where the company operates, resulting in a significant impact on operating models.

Data governance processes and technology are rapidly evolving. Boards will want to understand whether management is seeking opportunities to modernize, standardize, and automate processes. These changes can bring efficiencies and data quality improvement, and aid compliance with existing and new security and privacy laws. Boards will also want to know if the company has appropriate resources both in funding and talent to manage this important area.

Who oversees the data and privacy strategy?

With the data and privacy strategy aligned to the overall business strategy, the full board will want to get periodic updates on it. The board committee that oversees cybersecurity may play a role in overseeing data protection and compliance with laws and regulations, but this committee may not oversee the full breadth of the data strategy. Boards will want to discuss their approach and clarify how this important area is being addressed and who from the management team are best positioned to provide appropriate information.

Data governance also includes considerations of third-party risk. Companies use many third parties to help operate their businesses, and they may share or sell some of the personal or sensitive data they collect with these third parties. A robust third-party risk management program should uncover the scope of the risk posed by these parties—and whether the controls and processes in place are adequate to protect the data and comply with privacy regulations.

Conclusion

A holistic data and privacy strategy that addresses data value and related risks, combined with a thoughtful governance approach, can help the board and management create a competitive advantage and build greater trust with stakeholders.

How PwC can help

To have a deeper discussion about how this topic might impact your business, please contact your engagement partner or one of the PwC specialists below.

Maria Castañón Moats
Leader, Governance Insights Center
maria.castanon.moats@pwc.com

Barbara Berlin
Managing Director, Governance Insights Center
barbara.berlin@pwc.com

Joseph Nocera
Cyber, Risk and Regulatory Marketing Lead Partner
joseph.nocera@pwc.com

Jay Cline
US Privacy Leader, Principal
jay.cline@pwc.com