ISSUE 149
BOARD PERSPECTIVES

FRAMING THE DATA PRIVACY DISCUSSION IN THE BOARDROOM

Data proliferation and data privacy regulatory activity across the globe have created the need for focused boardroom discussions.

While cybersecurity continues to be an issue for boards, a more targeted focus on data privacy is increasingly necessary to ensure compliance across a rapidly expanding number of privacy regulations. Privacy risk represents a unique challenge driven by the volume and type of data an organisation captures and retains. The evolving regulatory environment, and changes to business and technology, further complicates this risk. The takeaway for directors: be familiar with the key components of data privacy and prepared to ask the right questions.

Privacy regulations focus on proper handling of personal data (data connected to an individual), which may include protected health information, Social Security numbers, bank accounts, medical histories and other classes of protected information of varying designations and regulated by various bodies and jurisdictions. The definition of personal data is also broadening as new technologies and data are created and collected. Whatever its composition, directors should inquire of and discuss with management the proper governance over personal data for collection, use and protection in accordance with applicable laws and regulations. As more data is collected, purchased, transformed, stored, shared and monetised, this task becomes more challenging.

protiviti®
Global Business Consulting

Directors should position themselves to participate in boardroom discussions with executive teams and the company's cyber and data privacy professionals regarding data governance and information security matters as regulatory scrutiny, the risk of cyberattacks and consumer demands for privacy protections continue to escalate. To that end, below are eight topics relevant to the boardroom conversation around data privacy.

Do we know what data we have and where it is? In addition to knowing what their "crown jewels" — the enterprise's most important information-related assets — are, organisations need to understand what personal data they hold, that appropriate privacy controls are in place, and that the data may either qualify for data subject access or deletion requests or have disclosure obligations. This conversation often leads to a realisation that data should be inventoried, catalogued and stored in a manner — whether structured or unstructured — that allows the organisation to determine whether the data is subject to privacy requirements in the jurisdictions in which it operates.

There should also be clear documentation and understanding of how personal data is collected and used in accordance with both the organisation's disclosures in its privacy notices and applicable regulatory obligations. In addition, appropriate security controls should be implemented based on risk, such as access controls and encryption techniques.

Recurring data inventory and classification assessments are standard best practice for all organisations storing personally identifiable information. Directors should ask management how the organisation leverages external parties to validate that appropriate privacy-related controls are in place. As the external auditors may force this conversation, management should be prepared by inventorying high-risk data inside the organisation and determining that protected data is properly inventoried, secured, shared and disposed of as required by regulation or determined risk.

Do we have a clear view as to why we acquire and retain data? Directors should understand the organisation's business purpose in collecting information, the collection process itself and the notice communicated to customers for the use of data. The "why" is just as important as the "what." Some questions directors should consider include:

- Is the company limiting data collection and retention only to the specific data points needed to drive its strategy while ensuring compliance with applicable privacy laws and regulations?
- How does the company acquire and use the information it collects?
- Are there industry-specific factors to consider, e.g., healthcare providers and financial institutions have specific data collection and management requirements?
- Has the company reviewed its policies and processes directed to the various media channels through which it engages consumers (however the company segments them)?

Thus, the organisation's mission and values have a bearing on the data it obtains. This conversation can lead to policies that place guardrails around data collection to manage data privacy risk. This is another area that may warrant a professional review.

Are we on top of the compliance requirements to which we are subject? Currently, there are at least 62 countries that have implemented, or are in the process of developing, their own privacy rules or mandates. So, there are privacy laws all over the planet — including in many U.S. states. To comply with emerging, unique privacy requirements in multiple jurisdictions, increased investment is likely required in addition to specialised talent to ensure that business processes are compliant.

Boards should inquire how in-house or outside legal counsel is sharing responsibility (and documenting evidence) across the organisation for staying abreast of evolving privacy laws and expanding their knowledge of data privacy requirements in the jurisdictions in which the organisation

operates. Based on the applicable laws identified, directors should understand management's strategy for managing myriad, complex and ever-changing global privacy requirements. The strategy will often determine where privacy risk lives within the organisation and investment is needed. A further complicating factor is that case law is evolving rapidly, which may expand the risks and penalties to organisations and directors. Therefore, continuous evaluation of the organisation's privacy strategy is required.

Are our legal agreements aligned with data protection requirements? Transferring personal data across international boundaries is becoming more difficult. While some jurisdictions require that personal data stay within certain regions, others allow personal data to transfer to other regions if certain legal obligations are met.

Directors should inquire, for example, whether the company is using the standard contractual clauses (SCCs) pre-approved by the European Union (EU) pertaining to the sharing of data between EU and non-EU countries.[1] These clauses provide standard terms and conditions to which both the sender and the receiver of personal data agree, with the objective of considering and upholding the rights and freedoms of the individual. Adopting these SCCs is a regulatory requirement for exchanging data with EU countries and is enforced by the European Commission. The board should also ensure that the agreements within the contractual clauses are not just agreed to but are operationalised and adopted.

How are we protecting the personal data of our consumers, employees and third parties? A key component to privacy risk management is the protection of personal data that an organisation holds. The level of sophistication of adversarial parties trying to access information has risen dramatically over the years, including carefully orchestrated, deceptive phishing tactics, distribution of data on the dark web and advanced persistent threats.

The prevalent trend in the marketplace is to utilise zero-trust architectures to ensure secure access to everything by everyone all the time. The idea is to shift cyber controls closer to the data that the organisation must protect, a notion that is fit for purpose in addressing the complexities of today's digital customer and supplier interactions, hybrid work environments, ever-expanding data protection requirements, and increasingly sophisticated cyber and ransomware attacks.

Practices becoming more pervasive over time include:

- Implementing strong "continuous verification" authentication technology
- Segmenting network access to reduce attack surfaces to limit the "blast radius" in the event of a breach
- Verifying end-to-end encryption and continuous network monitoring
- Applying least-privileged access by permitting only minimum privileges when granting access to data and applications
- Implementing privacy-by-design and cybersecurity-by-design methodologies that encourage proactive integration of privacy regulation and data management

From the board's standpoint, the intention is to achieve the strongest privacy protections possible.

[1] The "Standard Contractual Clauses (SCC)" pre-approved by the European Commission (June 4, 2021) are available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

From a privacy compliance standpoint, do we know what our stress points are? Notwithstanding that data privacy is a priority, businesses face obstacles when it comes to compliance preparedness. Lack of time and bandwidth, followed closely by the complexity of laws and regulations are examples.

Boards should encourage management to identify the trouble spots for privacy compliance, assess their severity and apply best practices to enhance the privacy program. This conversation may entail an assessment of the sufficiency of budget and resources as well as accountability for results. Stress-test protocols, tabletop exercises and the insights they provide are also of interest to the board.

Do we know how well we're doing in managing data privacy? Myriad privacy tools are becoming available that can provide confirming metrics that measure access to and usage of consumer personal data and enterprise privacy governance. These tools can help executive teams and their boards understand and effectively communicate an organisation's performance against its strategic objectives. Key performance indicators on the CEO's and board's dashboard are an imperative, but the quantity of tools may present a challenge. Going forward, companies are likely to streamline their current automated systems and models through significant consolidation of tools and rely on fewer tool vendors, creating more sustainable processes and reporting.

There is also the reputational impact of environmental, social and governance (ESG) reporting. Such reporting is likely to sharpen the focus on measuring an organisation's data protection capabilities as companies are increasingly evaluated based on their ESG ratings. That's why policies directed to internal reporting, external disclosure of breaches, and clarifying the financial and reputational impact from the loss of consumer and employee personal data merit the board's attention in fulfilling its duty of care responsibilities.

How should the board engage management on data privacy matters? The pervasiveness of data creates a challenge for boards. Multiple functions are accountable for the privacy and security risk of the data their activities collect, use and store, e.g., information technology, cybersecurity, human resources, legal and compliance. Some boards have a technology committee that reviews data privacy matters. Others assign these matters to the audit committee, and still others, in a highly regulated environment, to a compliance committee. For public companies, these matters merit consideration in every formal meeting of the committee that advises on data privacy, or more frequently as necessary — which underscores the importance of putting effective analytics and dashboards in place.

Companies with substantial business-to-consumer operating models will require more attention to these issues. The full board should be privy to a report or briefing on data privacy performance at least annually. Directors should engage the company's leadership with the intention of gaining confidence that a coherent data privacy governance process is in place, aligned with the business strategy and complemented by effective controls enabling data privacy protections.

The above topics and questions should be contemplated by the board, considering the risks inherent in the company's operations.

How Protiviti Can Help

Organisations around the world are experiencing unprecedented change in the data privacy landscape. Evolving state, federal and global regulations are forcing almost constant business, technical and legal operational adjustments. These changes aren't necessarily exclusive of one another and often overlap, resulting in highly complex legal and regulatory scenarios.

Protiviti's data privacy consulting team understands the inherent risks and challenges our clients face in developing and maintaining effective privacy and data protection programs. Drawing on our skills and experience in regulatory compliance, business processes, technology, information security and communications, we partner with our clients to understand jurisdictions and obligations, assess needs, implement appropriate compliance measures and safeguards, and respond to new and changing regulations.

protiviti®