protiviti®

Face the Future with Confidence

Responsible Privacy: Is the Board Doing Its Part?

Much has been said about the matter of privacy, even to the point of some directors developing fatigue for the topic. Nevertheless, each board needs to pay attention to this rapidly evolving area and the impact it has on the company's business model.

To gain fresh perspectives on this important area of board oversight, Protiviti met with a group of active directors during a dinner roundtable at a June 2019 National Association of Corporate Directors (NACD) event to discuss their experiences. Below are some of the important points covered, including key takeaways, during that discussion. (Note that an abbreviated summary of this roundtable is provided in Issue 120 of *Board Perspectives: Risk Oversight* [available at ***www.protiviti.com/US-en/insights/bpro120***] and on *NACD|BoardTalk* [see blog at ***https://blog.nacdonline.org/authors/42***].)

Recognize That Privacy Programs Are Stressed

Drivers of change are pressure-testing data privacy compliance programs and creating a complex legal matrix for companies to navigate. Factors of change include:

- ***Increased privacy regulations:*** With the meteoric rise of data proliferation worldwide has come new privacy laws such as the General Data Protection Regulation (GDPR) in the European Union (EU) and various derivative laws either on the books or on the way at regional, national and state levels (e.g., the California Consumer Privacy Act [CCPA]).
- ***Emerging technology:*** The rapid pace of emerging technology development and implementation is not only impacting existing information technology infrastructure but also compliance management systems. New technologies are exposing organizations to additional and possibly unanticipated risks.
- ***Consumer control:*** Consumers are now calling the shots. New privacy laws give them control over whether and how companies can use their personal data. Companies face significant risks by failing to effectively manage consumers' data directives. It's a new game with exposure to severe penalties if not played by the rules.
- ***Growth of vendor networks:*** More companies are using more vendors, creating exposure to greater risks as they manage extended global networks of suppliers, contractors, consultants and other third parties with access to protected and regulated data.
- ***Globalization and localization:*** Organizations now reach customers and clients worldwide with ease. But the technologies enabling this outreach create risks; moreover, the multitude of privacy laws worldwide crosses borders, creating a complex, far-reaching legal matrix to navigate.

These key drivers have redefined what privacy means for organizations today, sharpening the focus on corporate responsibility.

In considering how relevant privacy issues are affecting organizations and are most relevant to board members, one need only start with the class-action lawsuits these issues spawn. Two themes have emerged from these suits. First, the suit alleges that the board did not exercise the appropriate oversight. Second, the defendant

company's filings with the U.S. Securities and Exchange Commission disclosed that appropriate security and privacy practices were in place, but the court ruled that they, in fact, were not.

For example, in Illinois, a little-known law was introduced in 2008 called the Biometric Information Privacy Act. This legislation required written consent to collect biometric information from consumers; however, organizations using biometric devices were not complying with the law nor were authorities enforcing it. After a consumer learned of this issue and filed a class-action lawsuit, many more lawsuits followed. The result was class-action suits filed at a rate of four to five per day. Initially set at $1,000 per consumer incident, the legal settlement for many organizations amounted to $500 per consumer incident — a hefty sum when one does the math. In this instance, the key question was whether proper consent was obtained.

A question was raised by one board member as to whether there had been any movement by the U.S. Congress or the federal government to standardize privacy laws and regulations. To date, Congress has expressed no intent to do so, leaving such regulation to each state in recognition of states' rights. While action at the federal level is possible down the road, it is not likely in the near term. In addition, regulatory authorities likely want to see the CCPA as a testing ground and expect to assess its outcomes over the long term.

There also were questions from the directors regarding possible litigation from GDPR violations. Eyes are on the EU's treatment of a high-profile technology company that, at the moment, is facing a potential €1.6 billion fine for data and privacy practices that are allegedly not in compliance with the GDPR.

> ***Key Takeaway:*** Directors and management should be cognizant of the increasing intricacy of the privacy and security environment, especially given the increasing power of consumers and vigilance of regulators. To meet data privacy regulations and statutes, irrespective of whether they are required by the United States or the EU or by Brazil, India or other countries, the board needs to provide the necessary oversight to ensure management understands the environment and determine its implications to the company's business model. Boards should foster the appropriate coordination and support for the following business leaders and operational groups to stay current with and meet the most recent data privacy regulations: the chief information officer, general counsel, designated compliance officers and business unit leaders. It's not *someone's* job; it's *everyone's* job. Understanding the data and how it should be processed to comply with the various regulations and the gaps with how it is currently being processed requires this kind of collaboration. Accordingly, the board must ensure that management has engaged the appropriate parties within the organization to work together to create and sustain a shared and comprehensive data privacy solution.

Ask the Right Questions

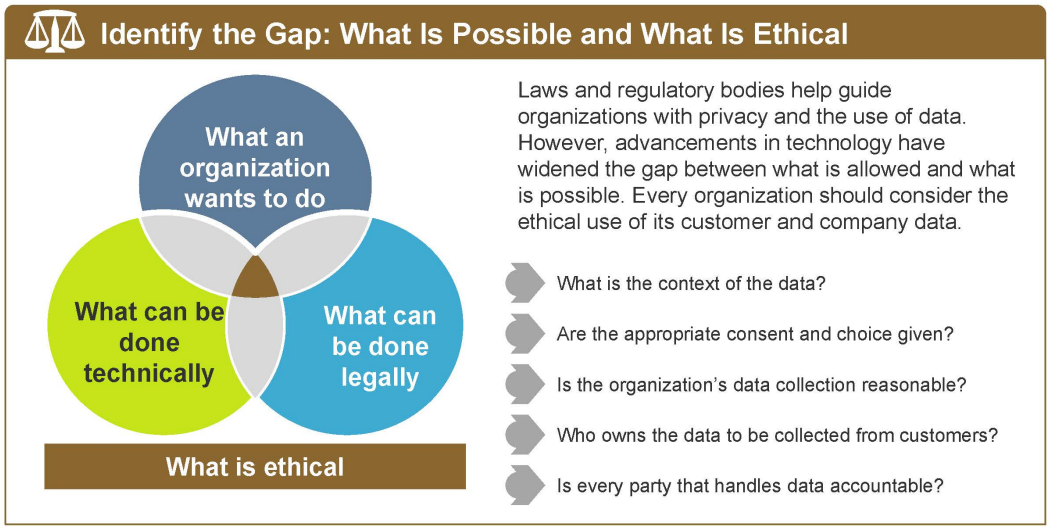
From a data and privacy perspective, boards are wrestling with understanding not only what is legal but also what is ethical and aligns with the company's brand. Compliance according to the letter of current privacy laws is one standard. Understanding to what extent data and privacy are an integral part of the organization's corporate strategy and business model, and how management defines what is an appropriate use of consumer/customer data, is a different and higher standard. The participating directors at the roundtable agreed that the board's primary role is to inquire and understand how management has defined these issues

and, in the process, obtain clarity on the desired risk profile and appetite regarding data collection and management and the related responsibilities accruing to the organization.

As for the board, the old cliché that directors must ask the right — and difficult — questions applies here as well. Board members should ascertain from management the processes the organization has in place to comply with applicable privacy laws in applicable regional, national and state jurisdictions, as well as potential new regulations that could go into effect in those jurisdictions. For example, while currently the United States does not have any federal laws governing data privacy that can compare to the GDPR (other than laws aimed at specific industries, such as healthcare and financial services), many states have been addressing this responsibility on their own. This dynamic has created a plethora of state privacy requirements, raising the question as to whether management is on top of them.

Another line of inquiry to management suggested for boards is how data is being used to drive and enable the execution of corporate strategy, as well as how the strategy itself shapes the methods by which the organization collects and uses customer data. Without intruding on management, the board should have a process to monitor how the organization is using and maintaining its data while ensuring compliance with privacy laws.

During the roundtable, there was a lively debate regarding the board's role in advising management on balancing compliance with privacy laws versus behaving in an ethical manner. Directors need to understand from executive and other management how they know the organization behaves ethically with regard to privacy and data management.



Source: Adapted from "Data Protection Law and the Ethical Use of Analytics," Paul M. Schwartz and "Ethics for big data and analytics," Mandy Chessell.

For example, there were many comments from the directors about the ethics and appropriateness of collecting, using and selling consumer data — behavior culminating from many years of commercial activity with the objective of monetizing data. Is this practice acceptable? How does it align with the organization's corporate strategy? What compliance issues present themselves from engaging in such practices? Where does the organization draw the line? Boards should understand the answers to these questions and their strategic underpinnings.

The discussion also noted that data collection and management, as well as compliance with privacy regulations, may be less of an issue for B2B organizations given that they are likely not managing large data sets of consumer information. However, boards serving these companies still need to determine whether management understands if and where consumers are touched as part of ongoing data collection and management processes. Only by doing this will they understand where the risk with that data is sourced.

Key Takeaway: There was much discussion in the room about privacy issues and ethics in general. With regard to privacy, board members need to consider three important, interrelated issues — compliance, ethics and corporate strategy. To that end, directors should consider the following:

- How is the organization dealing with the diverse standards that exist globally and, in some cases, nationally? How effective are the company's compliance processes in meeting current data privacy regulations?
- Compliance with privacy laws and regulations aside, what is "responsible" privacy practice, given today's optics and for the organization specifically? Is managing and using the company's data about ensuring regulatory compliance or doing the right thing or both?
  - What are the company's mores, policies and standards with regard to securing and leveraging the data of its customers?
  - Is there an alteration of the idea of privacy today? Is privacy strictly an issue of compliance for companies to address, or is ensuring privacy more than just complying with current laws? In other words, is privacy also about legitimate and ethical practices among companies?
- As part of the corporate strategy, what types of data usage are permissible in the organization? What policies and boundaries are in place to prevent improper usage of sensitive data?

Be Proactive

The board must understand what responsible privacy means specifically for its organization. As one director noted, boards need a standard — that is, a "North Star" — with regard to overseeing the organization's data and privacy management. Directors must have a clear understanding regarding data and privacy with regard to the balance between risk (protecting the organization) and strategy (innovation and growing the organization).

Key Takeaway: The boards that are most effective in working with management to understand and address data and privacy issues are proactive in their oversight rather than reactive. As both the United States and the rest of the globe continue to undertake significant policy changes with the resultant increases in data privacy obligations, an effective approach to data privacy is creating a compliance program and approach that meet the data privacy requirements of today *and* the future. Accordingly, directors should question not only how the company's compliance processes meet current data privacy regulations, but also whether they are flexible enough to meet future data privacy obligations. We do not believe this approach is as difficult as it seems, as most global privacy laws follow common principles that can be addressed in a consistent framework.

Understand the Business Purpose

With regard to emerging technology, the directors agreed that the board needs to work with management to understand the technology the organization uses to grow its business and, in the process, learn how it plans to use the data it collects — for example, marketing, business development, monetization or other purposes. Specifically, the board should understand from management what the business is doing with the information it collects, the risks arising from how data is collected and maintained, and how those risks are being managed.

In understanding the business purpose of collecting information and how the collection process and the use of data are being communicated to customers, it's also important for directors to inquire if the organization really needs all of the information it is collecting. Is the organization trying to collect everything it can get? Or is it limiting data collection and retention only to the specific data points it needs to drive its strategy while ensuring it complies with applicable privacy laws and regulations?

There may be industry-specific considerations as well. For example, there are unique considerations for healthcare provider organizations regarding data collection and management. These considerations make it important to understand the mission and values of the organization. To illustrate, a director cited an example whereby, while complying with current privacy laws, a healthcare organization might collect and end up selling/monetizing data in order to drive revenue that would enable it to acquire leading-edge healthcare equipment and technology as part of its overall mission to save lives. The group's debate was interesting: The organization is using data in a way that some may believe is not ethically appropriate, yet the organization's strategy is about saving lives by using the most advanced practices and technologies available. Driving revenue by monetizing data can help them achieve this mission. However, at the end of the day, the organization may be collecting and selling this information in a way that is inappropriate.

> ***Key Takeaway:*** The focus on purpose is ultimately about answering the question, "How much data is too much data?" Does the organization place guardrails around data collection to manage its risk? Or does it collect all of the information it can, understanding that there may be opportunities to monetize that data in some way, provided the company is complying with applicable laws and regulations? If this is done, is this return on investment (ROI) from the monetization effort sufficient to make the trouble in collecting and managing the data and the related risks worthwhile? But even if it is worthwhile, is this ROI from the monetization of data collected really integral to the strategy for driving shareholder value?

Look Outside the Organization

Boards also need to ensure that management understands where the critical data resides, and how it is being managed, both within the supply chain and among third-party providers. As most organizations know, the process can be outsourced but not the risks. Therefore, privacy and data issues arising with any third party — whether first-, second- or third-tier suppliers; outside processors of personally identifiable information (PII); or some other external party — still look back to the source for ultimate responsibility. That means any given company and its brand are ultimately liable for damages should its third-party vendors experience a data issue. That is why it is critical to ensure all third parties are operating consistently with the same privacy standards and maintaining data in compliance with the contracting organization's policies.

Key Takeaway: Third-party risk management is absolutely critical, especially with data management. It affects the entire value chain. Organizations failing to perform effective third-party risk management could face serious data and compliance issues. The board should obtain assurances from management, with the appropriate level of support, that the right vendor and third-party risk management and oversight processes are in place.

Examine Data Aggregation Practices

In the discussion, it was noted that data aggregation is another ethical and legal issue that organizations potentially face, particularly if they sell access to that data to other organizations. The collection of individual data is different from the aggregation of data, where individual consumer data and privacy may not be impacted. If data is scrubbed and cannot be attributed to a specific individual, is this acceptable?

Consider a healthcare organization that is collecting and testing blood samples. Is it appropriate for that organization to use the data from the blood samples and markers to aggregate and understand broader trends, and even make that aggregated data available to other healthcare organizations?

Boards need to work with management to define the activities and parameters around data aggregation and ascertain whether the organization's risk profile may change (e.g., risk may be increased or reduced) as a result. There also are different ethical considerations involved, as aggregated data may no longer contain PII or legally protected consumer information. Accordingly, the board should understand the organization's strategy and practices regarding data aggregation in the context of the company's agreed-upon views on ethics, compliance and the desired risk profile.

Key Takeaway: Is data aggregation the right thing to do? How effective is the company's process for aggregating data in maintaining compliance with privacy laws and regulations? Is the data being scrubbed and anonymized appropriately? These and other considerations underscore the importance of understanding the company's values, ethics, process and purpose in using data the organization collects. Ultimately, boards need to work with management to understand whether data aggregation and usage practices are appropriate for the organization to undertake.

Questions for Boards

Based on the risks inherent in the entity's operations, has the board considered the key takeaways noted in the above discussion?

How Protiviti Can Help

Protiviti is a global organization that supports our clients' data privacy programs in numerous countries. Whether in the United States with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the California Consumer Privacy Act (CCPA) or other state- or federal-based regulations, the EU with the General Data Protection Regulation (GDPR) or the future EU ePrivacy regulations, the individual EU member states, or other countries such as Brazil, India, China and Canada, Protiviti helps companies create effective and efficient data privacy approaches. We support privacy and security by assessing readiness, helping businesses better understand their data privacy posture and designing cost-effective compliance solutions covering the people, processes and technologies needed to help drive sustainable and effective privacy programs.

We work cross-functionally with groups such as IT, legal, compliance, marketing and business units to develop, implement and help maintain national and globally focused data privacy compliance programs. Our services include:

- **Regulation interpretation —** analysis and advice;
- **Advanced data management techniques —** including automated data and processing discovery;
- **Gap remediation with leading practices —** including design and implementation of third-party risk, data privacy rights, data governance and privacy notices;
- **Compliance solutions —** integrating people, process and technology execution for an effective cybersecurity and privacy program; and
- **Compliance management —** monitoring and maintaining controls going forward.

We support clients during all stages of their compliance efforts. Our organization integrates global consulting talent from our different practices and backgrounds to provide a customized team to address our clients' international data privacy needs, including functional expertise from our Global Security and Privacy practice and our Data and Analytics teams, as well as legal and privacy support from Robert Half Legal.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 75 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Contacts

Greg Reid
Privacy Practice Global Leader
+1.617.646.2705
greg.reid@protiviti.com

Jeff Sanchez
West Region Technology Consulting Leader
+1.213.327.1433
jeffrey.sanchez@protiviti.com

protiviti®
Face the Future with Confidence