ISSUE 120

BOARD PERSPECTIVES: Risk Oversight

RESPONSIBLE PRIVACY: IS THE BOARD DOING ITS PART?

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

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 in this area. Below are some of the important points covered during that discussion, including key takeaways.

Recognise That Privacy Programmes Are Stressed: Drivers of change are pressure-testing data privacy compliance programmes and creating a complex legal matrix for companies to navigate. Factors of change include increased privacy regulations, emerging technology, consumer control over the use of personal data, growth of vendor networks, and the forces of globalisation and localisation. These drivers have redefined what privacy means for organisations today, sharpening the focus on corporate responsibility. They are spawning class-action suits alleging that the board didn't exercise appropriate oversight and the company's public reports disclosed that appropriate security and privacy practices were in place when, in fact, they were not.

Key Takeaway — Directors and management should be cognizant of the increasing intricacy of the privacy and security environment and determine its implications to the company's business model. Boards should foster the coordination and support for the following business leaders and operational groups to stay current with and meet the most recent regulations: the chief information officer, general counsel, designated compliance officers and business unit leaders.

protiviti®

Face the Future with Confidence

Ask the Right Questions: From a data 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 privacy is an integral part of the organisation's corporate strategy and business model, and how management defines the appropriate use of consumer 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, clarify the desired risk profile and appetite regarding data collection and management and the related responsibilities accruing to the organisation.

> **Key Takeaway —** The old cliché that directors must ask the right — and difficult — questions applies here as well. 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 organisation 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 organisation specifically? Is managing and using the company's data about ensuring regulatory compliance, 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? How should the board's oversight role address these areas?
- As part of the corporate strategy, what types of data usage are permissible in the organisation? What policies and boundaries are in place to prevent improper use of sensitive data?

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

> **Key Takeaway —** The boards that are most effective at working with management to understand and address data and privacy issues are proactive in their oversight rather than reactive. 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.

Understand the Business Purpose: On the topic of emerging technology, the directors agreed that the board needs to work with management to understand the processes and technology the organisation uses to grow its business and, in the process, learn how it plans to use the data it collects — for example, marketing, business development, monetisation 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 managed. In understanding the business purpose of collecting information and how the collection process and the use of data are communicated to customers, it's also important for directors to inquire if the organisation really needs all of the information it is collecting.

Key Takeaway — The focus on purpose is ultimately about answering the question, "How much data is too much data?" Does the organisation 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 monetise that data in some way, provided the company is complying with applicable laws and regulations? If it is the latter, is the return on investment (ROI) from the monetisation effort sufficient to make the trouble of collecting and managing data and the related risks worthwhilst? And if so, is this ROI from the monetisation of data collected integral to the strategy for driving shareholder value?

Look Outside the Organisation: Boards also need to ensure that management understands where critical data resides, and how it is managed, both within the supply chain and amongst third-party providers. 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 organisation's policies.

Key Takeaway — Organisations that fail 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: The roundtable discussion noted that data aggregation is another ethical and legal issue that organisations potentially face, particularly if they sell access to that data to other organisations. The collection of individual data is different from the aggregation of data, which may not impact individual consumer data and privacy. Boards need to work with management to define the activities and parameters around data aggregation and ascertain whether the organisation's risk profile may change 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 organisation'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 anonymised appropriately? These and other considerations underscore the importance of understanding the company's values, ethics, process and purpose in using data the organisation collects.

For a complete look at this roundtable, including more key takeaways, read Protiviti's comprehensive summary of the event at www.protiviti.com/US-en/insights/responsible-privacy-board.

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 organisation that supports our clients' data privacy programmes 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 European Union (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 programmes.

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 programmes. 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 programme; and
- **Compliance management** — monitoring and maintaining controls going forward.

We support clients during all stages of their compliance efforts. Our organisation integrates global consulting talent from different practices and backgrounds to provide a customised 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.

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.

Protiviti partners with the National Association of Corporate Directors (NACD) to publish articles of interest to boardroom executives related to effective or emerging practices on the many aspects of risk oversight. As of January 2013, NACD has been publishing online contributed articles from Protiviti, with the content featured on https://blog.nacdonline.org/authors/42/. Twice per year, the six most recent issues of *Board Perspectives: Risk Oversight* are consolidated into a printed booklet that is co-branded with NACD. Protiviti also posts these articles at protiviti.com.

protiviti®