KPMG

Data governance should be part of your boardroom conversations

KPMG Singapore Board & Governance Institute

Today we are seeing the convergence of cybersecurity and data governance. An array of business forces are impacting companies' risk posture and causing greater complexity in protecting their data assets. These forces include technological advances and the leveraging of big data, new privacy laws and regulations, customer expectations for privacy, the global extension of business, and more advanced cyberattack scenarios.

In our conversations with directors, we often hear that while companies and boards are making progress in their cybersecurity efforts, for many, there needs to be a more rigorous approach to data governance — the processes and protocols in place around the integrity, protection, availability, and use of data.

Cybersecurity has long been a top priority for boards. Based on our conversations with directors, it appears that boards have made significant strides in monitoring management's cybersecurity effectiveness. We are seeing, for example, greater information technology expertise on the board and relevant committees, company-specific dashboards that highlight critical risks, and more probing conversations with management on critical cybersecurity risks, operational resilience, and the strategies and capabilities deployed to minimise the duration and impact of a serious cyber breach. Despite these efforts, given the growing sophistication of cyber-attackers, cybersecurity will continue to be a key challenge for companies and boards.

While data governance overlaps with cyber-security, it is broader and includes a number of issues that should be top of mind for boards today, including compliance with data privacy laws and regulations, data ethics, and data hygiene.

Compliance with data privacy laws and regulations. In addition to industry-specific privacy laws and regulations, a number of new laws and regulations govern how the personal data of customers, employees, or vendors is processed, stored, collected, and used.

Examples include the European Union's General Data Protection Regulation, which took effect in May 2018, and Singapore's Personal Data Protection Act 2012 (PDPA).

The Personal Data Protection (Amendment) Bill 2020 was published on 14 May 2020 for public consultation. Various initiatives in the proposed amendment bill are directed at enforcement.

We can expect more privacy laws and regulations to follow, both in Singapore and internationally.

Data ethics. Beyond technical compliance with privacy laws and regulations, companies need to manage the tension between how they legally use customer data and customer expectations about how that data is used. This tension poses significant reputation and trust risks for companies.

Data hygiene. As one director suggested, the company should regularly ask: Are we collecting or holding data that we don't really need? If yes, get rid of it and perhaps stop collecting it. Who has access to the data, including vendors and third parties?

The convergence of cybersecurity and data governance presents a significant challenge for executive teams and boards. As one director said, "If data is such a critical asset, don't we need a more rigorous governance approach around that asset, similar to governance around financial reporting, which has clear roles for the chief financial officer and finance team; internal and external auditors; audit committee oversight; and audit committee financial experts, assessments of controls, etc.?"

To help develop a more rigorous approach around data governance, we recommend three areas of board focus:

- ❑ Insist on a robust data governance framework that makes clear how and what data is being collected, stored, managed, and used, and who makes decisions regarding these issues.
- ❑ Clarify which business leaders are responsible for data governance across the enterprise — including the roles of the chief information officer, chief information security officer, and chief compliance officer.
- ❑ Reassess how the board — through its committee structure — brings the right focus and attention to cybersecurity as well as the company's data governance framework, including privacy, ethics, and hygiene.

Adapted from article originally published in the November/December 2019 issue of NACD Directorship magazine. Contributed by Patrick A. Lee, Senior Advisor, KPMG Board Leadership Center.

Data governance should be part of your boardroom conversations

Contact us

Irving Low
Head of Board & Governance Institute
T: +65 6213 2071
E: irvinglow@kpmg.com.sg

Emilie Williams
Director
KPMG Asia Pacific
T: +65 6411 8007
E: emiliewilliams@kpmg.com.sg

KPMG Services Pte Ltd
16 Raffles Quay
#22-00 Hong Leong Building
Singapore 048581
T:+65 6213 3388
F: +65 6225 0940

kpmg.com.sg