BRC
BOARD RISK COMMITTEE

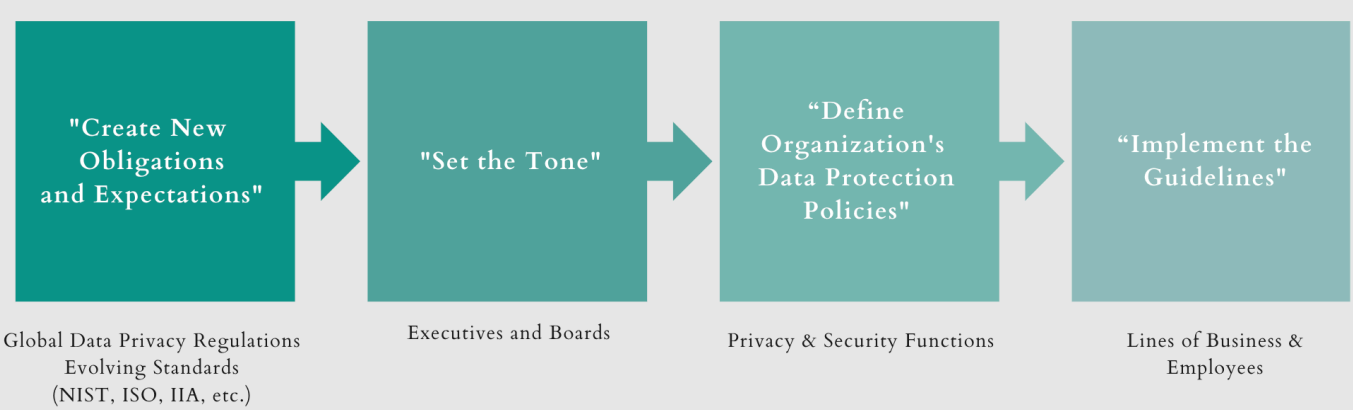
BOARD RISK REPORT

October 15, 2020

THE EMERGENCE OF DATA PROTECTION ENGINEERS

Compounding the current critical lack of cybersecurity talent is a scarcity of subject matter experts who have integrated privacy and data protection expertise. A new cohort of professionals with security expertise combined with a focus on data protection and data governance has emerged. These specialists can speak more effectively to privacy controls which can be quite nuanced and dependent upon business models and compliance triggers based upon range of privacy regimes under which they may operate.

Risk Management Model for Aligning Organizational Data Protection Functions



In response to this specialist shortage, NIST and IAPP launched an industry effort to align taxonomy, skills, and the knowledge required for managing both cybersecurity and data privacy risks.
The overarching objective of this collaboration is to define the tasks, skills, and workforce roles that drive effective coordination between privacy and cybersecurity disciplines.

Steps Boards and Risk Committees can take:

- Take steps to broaden the privacy team's technology knowledge, while advancing security team understanding of rapidly evolving privacy regulations in jurisdictions where your firm does business.
- Use cross-training that addresses shared responsibilities.
- Evaluate existing staffing models and identify personnel and organizational certifications that enhance the company capabilities to address growing data protection risks.
- Consider stronger integration of privacy requirements into the Software Development Lifecycle to build collaboration for both disciplines while mitigating data protection risks.

THE INCREASING IMPACT OF PRIVACY REGULATIONS ON BUSINESS OPERATIONS

The C-Suite and the Board must understand the increasing impact privacy enforcement actions may have on their business and ensure that privacy risks are mitigated as part of their overall approach to resilience.

As privacy regulations become more stringent and apply more broadly across jurisdictions and industries, it has become increasingly clear that organizations are challenged to achieve and maintain compliance. In fact, significant privacy compliance failures can result not only in substantial fines, but can directly impact business operations.

An important attribute of privacy regulations is the trend toward identifying specific requirements and enforcement obligations that are business model or service based - whether those functions are outsourced or not. EU data protection authorities have the right to inspect vendor contracts for adequacy and to disallow data transfers if appropriate data protection controls cannot be confirmed. In July, the EU Court of Justice invalidated the Privacy Shield, a certification that enabled streamlined data transfers between the EU and the United States. Companies and their vendors that relied on the Privacy Shield are now required to address data protection via standard contractual clauses and by conducting formalized risk assessments. Privacy disruptions can have immediate and long term revenue impacts as global momentum to increase the enforcement power of local data protection authorities accelerates:

- Failure to comply with a Brazilian Privacy regulation can now trigger blocking of the processing of personal data including placing a freeze on a company's web site with direct revenue implications for up to six months.
- Fines for failures to meet GDPR obligations have doubled in 2020, reaching 373 enforcement actions with aggregate fines exceeding $600 million. Further, EU Authorities can now require companies to discontinue data transfers outside their jurisdiction including requiring the selection of alternative service providers.
- Concerns over governmental access to information has created data localization trends for a range of digital device and smartphone application providers. Such restrictions have the potential to limit competition and increase the costs of providing services, impacting the bottom line.

Steps Boards and Risk Committees can take:

- Review existing business resilience programs to determine if privacy disruptions are included in Business Impact Analysis and recovery objectives.
- Bring together business continuity, crisis communication, and privacy/security personnel to conduct a table-top exercise or simulation to test the impact of a privacy disruption.
- Identify any third party relationships that relied upon the Privacy Shield as the authorized data transfer mechanism and update risk registers and vendor inventories to quantify impacts.

THE IMPACT OF THE BUSINESS MODEL IN PRIVACY REGULATIONS

The buildout of remote work force capabilities has redoubled a focus on the crosstalk between security and privacy requirements. In today's COVID-19 environment many organizations found they did not have an equivalent set of fully vetted privacy expectations to adequately distinguish between what they could do and what they should do to monitor employee behavior in remote environments. The reported speed in which companies had to enable remote workers and securely manage remote vendors altered the deployment of traditional cybersecurity controls.

In response to the perceived complexity of coherently integrating security and privacy into enterprise risk management processes, NIST created a roadmap for organizations to fully incorporate Privacy into their ERM Programs.

Boards and Risk Committees can direct management to utilize the combined roadmaps and cross-walks to data protection regulations to strengthen risk oversight and incorporate structured evaluation of controls across a defined set of privacy, cybersecurity, and data governance control frameworks.

Steps Boards and Risk Committees can take:

- Review the company's approach to addressing remote work requirements that require updated risk assessment, remediation, enhanced mitigating controls, or changes to permitted exceptions.
- Assess the level of privacy risk that is included in ERM programs. Confirm if ERM processes include the assessment of operational privacy risks beyond a strict regulatory perspective.
- Assess the maturity of existing data governance programs that encompass the management of data both within the boundaries of the organization and with external third parties.

ADDITIONAL SOURCES

NIST Privacy Framework
H&M Germany fined $41.3M in one of largest GDPR penalties
The enterprise imperative of cyber resiliency post-COVID-19
2020 Data Privacy Benchmark Study

"I thought, oh, I'd like to find out about what these companies know about me. Then I thought, well, someone should do something about that."

Alastair Mactaggart
Online Privacy Law Advocate

RESOURCES

The Need For Board Risk Committees Webinar Recordings

Women Corporate Directors and The Santa Fe Group partnered for "The Need for Board Risk Committees" webinar series. In these webinars, panelists address emerging operational risks, the value of Board Risk Committees, and what it takes to form one and follow best practices.

View Webinars

WHO WE ARE

The Board Risk Committee (BRC) is a non-competitive thought leadership peer forum dedicated to Board Risk Committee members and Chief Risk Officers (CROs). The BRC is a trusted place for the exchange of ideas, best practices, and topics of interest. BRC is affiliated with The Santa Fe Group (SFG). SFG is a strategic advisory company providing unparalleled expertise to leading financial institutions, healthcare payers and providers, law firms, educational institutions, retailers, utilities, and other critical infrastructure organizations.

CONNECT WITH US