Published By

NACD

Governance Challenges 2021–2022

DIGITAL TRANSFORMATION OVERSIGHT

Brought to you by

SIDLEY

The Time to Prepare Is Now: Privacy Requirements and Breaches Will Not Wait

Sidley Austin LLP

Privacy and cybersecurity concerns are expanding, and with them the proliferation of laws and regulations. Boards play a key role in ensuring that companies are positioned to comply with various jurisdictional requirements, that they understand and mitigate related risks, and that they are well-prepared to play a key role in response to security breaches and incidents. Indeed, enforcement actions issued by the US Securities and Exchange Commission in 2021—including penalties levied due to a lack of senior leadership awareness of the identification and response to security vulnerabilities—sharpened this focus and shed light on regulatory expectations of corporate board oversight relating to privacy and cybersecurity.

Recognizing that companies are at different points in this journey, boards should heed guidance on how to prepare for the ever-evolving landscape of privacy and cyber laws. Advice on oversight in this area follows and is directed at assuring boards that management is prepared to get ahead of potential breach issues and respond effectively when a breach or an incident arises.

DEVELOP OR EVOLVE YOUR PRIVACY COMPLIANCE PROGRAM

International companies are grappling with how to ensure a consistent and compliant approach to privacy and cybersecurity across their business. Doing so may seem daunting but looking at the process in steps helps to ensure that each unique consideration is addressed. At a basic level, addressing global privacy and cybersecurity compliance requires assessing the various regulatory requirements in different jurisdictions, the nature of the data, and the risks present for the company. However, regardless of the responses to each of these points, there are several core tenets of a privacy and cybersecurity program that span sound compliance practices. Below are steps and tips for how to approach global privacy and cyber compliance efficiently—a framework that can help your board to understand if its newly developed or evolving program meets best-practice expectations.

Assign Accountability and Determine Scope

As a first step in the development of any data privacy and cybersecurity compliance program, accountability should be assigned by leadership for who within the company is going to be responsible for developing, implementing, and validating the program going forward. For companies with established privacy functions, this responsibility will likely reside with the chief privacy officer (or equivalent). However, for companies with less sophisticated programs, consideration will need to be given to where this will best sit within the company. It is important to bear in mind that the development and implementation of such a program is no easy task and will require executive-level and operational support, and that the board may request reporting on the success of the program to fulfill its oversight duties.

Identify Data

The next step in creating the program is for operational teams to identify and document what data are being processed by the company, the nature of the data (e.g., sensitive, classified, solely business contact details, etc.), and for what purposes the data are being used. This step requires a comprehensive understanding by the company of the internal and external data flows within the business. In practice, some companies approach this manually (i.e., through interviews and questionnaires) and others leverage software. While software solutions can be time and resource intensive at the outset, they can increase efficiencies going forward (e.g., automating responses to requests from individuals to delete their personal data). Identifying the data will also be pivotal to addressing potential security incidents, allowing for a quicker assessment of the impact of new privacy laws and affording clearer insights when reporting to the board.

Determine Applicable Laws

The company will then need to determine which of the plethora of national, state, and local laws it is subject to, including in relation to which of its data processing activities. Consideration should also be given to the impact such laws have on the company's operations. For example, a company with all their servers in China will want to consider more closely the impact of China's new Personal Information Protection Law as compared to a company that may occasionally send limited personal data to a Chinese-based counterparty. The approach to be taken will largely stem from the risk appetite and culture of the individual company, as identified by the board and leadership.

Pulling the Pieces Together

Once the relevant laws have been identified, the collected information needs to be combined and reviewed by the appropriate teams to determine the program's requirements. A gap analysis should be carried out to compare the company's current practices against these requirements. It is at this stage of the project that the company should identify the potential risks (e.g., regulatory fines, litigation, reputational damage). This will enable the company to undertake a risk assessment and determine how it wants to approach various risks, and it will allow it to prioritize various remediation activities.

Tangible program deliverables are likely to include amendments or drafting of various policies and procedures, including those mandated under specific privacy and cybersecurity laws. The program may also require updates to vendor and customer contracts, as well as privacy assessments. A key component of the success of the program is for operational teams to ensure that personnel are familiar with the requirements and what their obligations are within the new policies. In turn, training coupled with an internal privacy awareness campaign are paramount. The board may consider requesting reporting from operational teams on the efficacy of these trainings and on compliance with policies as part of board-level oversight of the program's success over time.

Finally, companies should audit the program going forward and ensure that it remains effective and can adapt to the development of new laws. The report from this audit will allow the board to ask the right questions of management—questions that will draw out the kind of information the board needs to understand whether or not the company is on track.

Building Upon Existing Programs

As new laws emerge and evolve, it is common to expand upon current compliance programs to account for new jurisdictions. Because many laws borrow from each other, start by leveraging already undertaken activities and ongoing processes.

Directors should apply the same commonsense approach to cybersecurity risks that they apply to other risks, with a focus on the company's policies and processes.

Companies that have implemented a program for the EU General Data Protection Regulation may leverage that work to develop a business-wide, principle-based program across multiple jurisdictions. Similarly, companies in the United States may start with compliance efforts undertaken for the California Consumer Privacy Act when assessing compliance with new US state privacy laws. However, this approach does not preclude the need for international companies to consider the laws in each of the relevant jurisdictions as there are often nuances in such laws that will need to be considered in the compliance program.

THE BOARD'S ROLE IN THE PROGRAM

Once set in motion, boards have a general obligation to oversee the systems that management has put in place to identify, mitigate, and manage risks to the company's privacy and cybersecurity systems. Directors should apply the same commonsense approach to cybersecurity risks that they apply to other risks, with a focus on the company's policies and processes, including compliance programs, and attention to the appropriate deployment of corporate resources to educate themselves about the risks.

In general:

- The board should have a high-level understanding of the nature of the cyber risks facing the company from a business-wide risk perspective. The depth of understanding required will differ based on the industry and the company.
- Detailed technological understanding is not required by the board, but the board should be well advised and have access to relevant technological and legal expertise, as required.
- Discussions about cyber-risk management should be given regular and adequate time on the agenda of the full board and in committee meetings.
- The full board (with assistance from an appropriate committee) needs to understand and oversee the policies, controls, and procedures that management has put in place to identify, manage, and mitigate risks related to cybersecurity and to respond to incidents. This includes understanding—and, if necessary, setting expectations regarding—staffing and budget.
- Public-company boards need to provide oversight of related disclosures and disclosure controls and procedures.

Beyond and above these basic requirements, and those tied to the development of a privacy program, your board might be held accountable for the following oversight areas and for understanding certain terminology.

Differentiation Between Breaches and Incidents

While breaches were once thought of as uncommon and only impacting certain types of companies, the adage has become that it is not a matter of whether a company will be breached, but when. To this end, preparedness for a breach is paramount, and should include system controls and plans to address a potential breach when identified.

The time to build relationships (and contracts) with entities such as outside counsel and forensic providers should be spent before, not during, a security incident.

Terminology is key: both management and the board should avoid referring to an incident as a "breach" prior to the incident being confirmed as such as the term "breach" often has a legal meaning, and therefore legal implications. Instead, when first learning of a potential event, the term "potential security incident" is commonly used. Once the appropriate team confirms infiltration, "security incident" or a "confirmed security incident" are options.

Assign Accountability

Having key people in charge of different security efforts is very important to ensuring operational success and also when assessing and responding to a security incident. Security teams are typically a mix of roles, which will partly be determined by the nature of the data handled by the company and the respective operations related to that data. Having individuals who understand the different jurisdictional requirements and setups is also key for multi-jurisdictional companies. A team or individual who reports to the board can be a good way to create accountability. Demonstrating top-down interest, and also showing that leadership fully engages in cybersecurity, helps to ensure that consistent attention is paid to its success.

Create Program Materials

Using template materials or borrowing from another company is simply not sufficient to create a well-documented security program and will not adequately prepare a company for a breach or incident. While this type of approach may save money and time up front, the costs when a security incident arises will likely cancel out any earlier savings, and that does not include costs associated with potential litigation and reputational harm.

Boards looking to understand whether or not they have a proper program in place should account for the requirements aligned to different types of data, including where separate policies and procedures may be required. For instance, incident response plans should include participants from many different teams within a company, and sometimes outside advisors (such as outside counsel). Information security policies should be specific enough to be worthwhile and should be accompanied by training. Documents should result in clear plans that account for regional considerations, such as tight reporting time lines when acting as a data controller in the European Union, and an incident response plan should have a clear list of contacts for different needs, including how and when the board should respond—or not. The time to build relationships (and contracts) with entities such as outside counsel and forensic providers should be spent before, not during, a security incident. It is invaluable for these teams to already have relationships with these vendors, and preferably to have shared information about underlying company operations that would help speed the time to response should there be an incident. The board may consider asking management about the company's relationships with the necessary parties when conducting oversight of the program.

Build and Expand an Infrastructure

Boards should press to understand the risks associated with different budget and technology requests and they should remember that the longer something waits to be implemented to be compliant with a new regulation, the higher the likelihood that it will be more expensive and complicated to implement. Waiting may also have significant increases to risk. As mentioned above, having regular reporting from teams managing system security should help to ensure that a board is informed and able to make appropriate decisions.

THE WORK IS NEVER DONE

Once a good incident response plan and data privacy program have been put together, a tabletop exercise will help ensure that kinks are ironed out of the plan and that people—including the board—are ready for a real incident. Similarly, on-the-go security testing, such as mock phishing campaigns, are a good way to regularly monitor and help prevent employee-related security incidents. Further, monitoring ongoing news and industry reporting of new risks will be crucial to ensure that updates to the program are appropriately considered and implemented.

A successful privacy and cybersecurity program requires attention to systems and controls to ensure that they incorporate adequate safeguards to prevent or mitigate an incident. It also requires an understanding by employees, management, and the board of their respective roles in preventing and mitigating risks, and in the board's case, of their role in overseeing the systems and controls that management has put in place as well as their role in assessing its adequacy in relation to the risks facing the company.

NACD®

Empowering Directors. Transforming Boards.

1515 N. Courthouse Road, Suite 1200
Arlington VA 22201
nacdonline.org