CG NEWS UPDATE

OVERSEEING CYBER RISKS IN A COMPLEX REGULATORY LANDSCAPE

July 18, 2019 By David Ross

Organizations face increasing cybersecurity risks and threats to their customers, financial information, operations and other data, processes, and systems—and state and federal governments are alert to the threats imposed on their constituents. To understand just how widespread concerns about these risks are, look no further than the abundance of cybersecurity legislation that is currently on the dockets of state legislatures across the country.

For example, California, New Jersey, Washington, and Illinois are among the latest states to enact breach notification legislation that will significantly impact businesses operating in those jurisdictions by defining whether, when, how, and to whom notifications of a breach must occur. Some of these laws are going into effect just months after being signed and the cost of noncompliance can be severe (in California, fines are assessed per record breached).

As stewards of the strategy, finances, reputation, and overall direction of an organization, corporate directors have an important role to play in ensuring adequate policies and protections are in place to answer the demands of such regulations—and that their whole board is ready to meet the oversight demands of new regulations.

Directors are in a position to provide the leadership and strategic direction necessary to help their organizations balance the need to safeguard information, minimize disruption in case of an attack or breach, provide transparency, and manage a sustainable cybersecurity program with competing strategic priorities.

There are four key steps boards should take to ensure adequate cybersecurity program development and oversight in response to emerging regulations and threats:

1. Understand the threat landscape and how companies are expected to respond under the law.

Corporate directors and leaders need a clear picture of the threats at play to assess and implement an appropriate response framework that both meets the business's needs and is compliant with a complex web of laws.

Adversaries' tactics will vary based on their motivations. Nation-states may be focused on cyber warfare while garden variety criminals

CG NEWS UPDATE

(including internal threats) are likely to commit fraud or steal information. Each of these threat types will warrant their own response, and may also warrant involving different law enforcement and regulatory agencies.

It is also important to note that the nature of threats will vary by industry. A real estate company is likely to face a higher risk of wire fraud, while a manufacturer might be a target of theft of information by foreign governments. Directors should spend time in their busy schedules understanding the appropriate responses required per industry-specific regulations.

In addition, the range of threats—from phishing and social engineering to attacks on the supply chain—is constantly shifting. Boards must be aware of emerging threats, ensure they have the right team in place as first responders, and ensure people and processes are in place to help mitigate and address regulatory and compliance consequences from cyber incidents.

2. Ask relevant executives, leaders, and legal counsel the right questions.

The board is tasked with gathering information from leadership, but the value of the exercise is dependent on asking the right questions. This ability becomes much more acutely important in light of a cyber breach, but should be practiced early and often. While these types of questions have been suggested for review by many in the cybersecurity community, it is worth asking the following in light of increased regulatory action:

- On risk: What are our risks and how are they being mitigated? Who is the owner of a particular risk?
- On capabilities: What are the people, tools, and processes we have in place to implement our cybersecurity framework? Do these comply with the demands of new and existing regulations?
- On controls: What controls are currently in place? What are the organization's cybersecurity policies and procedures (e.g., incident response plan) and when were they last reviewed, tested, and updated? What training do employees receive regarding privacy and security?
- On trends: What industry-leading best practices should be considered? What stories of disaster should we read and learn from?
- On regulation: What is taking shape at the local, state, and federal levels that will impact the business? What is the plan to get compliant and stay compliant?

CG NEWS UPDATE

2. Ask relevant executives, leaders, and legal counsel the right questions.

In the event of an attack, it will be important to demonstrate to regulators good faith efforts to identify and remedy risks. The extent to which an organization can show regulators that they did the work up front and put controls into place based on industry standards and best practices will determine the strength of their case for reduced penalties. For most organizations, cybersecurity incidents and regulatory noncompliance are associated with legal, financial, and reputational risks.

Compliance and risk mitigation come with their own set of financial costs. In Arizona, the maximum fine is $500,000 per breach event while Alabama can impose a fine of $5,000 per day for failure to comply with its notification law. To make decisions about risk tolerance, companies need to balance the risk with the cost of everything from business interruption to notification costs and potential fines.

Directors of companies should also closely review their own director and officer liability insurance policies frequently to see if cyber-risk-related incidents are covered.

4. Establish metrics for governance.

One of a board's most important roles is to establish and assess metrics to enable oversight of the company's cybersecurity program. The board should prioritize the development of a well-documented plan that is designed to account for and address evolving regulations, including a board-level metrics portfolio focusing on the following categories:

- Program status, including cybersecurity strategy milestones and program tracking;
- Internal environment updates such as patching and the state of infrastructure, and the capacity of people to prevent phishing and data loss;
- External environment updates, including the ability to gather threat intelligence and respond to emerging cyberthreat trends;
- Compliance and audit figures on cybersecurity audit planning and regulatory compliance tracking; and
- Response figures on disaster recovery, business continuity, and incidence response planning.

Board members' oversight of cybersecurity programs is crucial to protecting business interests from current and future threats.

CG NEWS UPDATE

This requires boards to take an active role in strategy, validation, detection, and response plans, ultimately steering the dialogue with stakeholders to better understand, assess, and identify cybersecurity needs and deficiencies that need to be addressed.

It is impractical and inefficient for organizations to revamp their cybersecurity risk management program each time a new law goes into effect. Organizations with a presence in multiple jurisdictions should instead think holistically about their programs. With the cyberthreat landscape constantly changing, it requires that risks be regularly weighed against strategic goals—and that the company meets the regulatory demands created to protect businesses and consumers alike. By ensuring the quality of a company's cybersecurity framework through leadership and oversight, a board can fulfill its obligation to protect the overall health and sustainability of the organization.

Ref.
https://blog.nacdonline.org/posts/cyber-risks-regulatory-landscape